NORTEL NETWORKS

Enterprise Edge Networking Operations Guide

1-800-4 NORTEL
www.nortelnetworks.com

© 1999 Nortel Networks
P0910464 Issue 01

Contents

Chapter 1 Introducing Enterprise Edge 7

Routing and IP Services 7
- System Software 8

Chapter 2 Using Enterprise Edge Unified Manager 9

Understanding Unified Manager 9
- Changing the appearance of Unified Manager 12
- Adjusting Unified Manager views 12
- Navigating between views 13
- Changing column order 14
- Generating statistics 15

Menu descriptions 16

Chapter 3 Using Enterprise Edge Services 17

Enterprise Edge required parameters 17

Setting up an Enterprise Edge IP Address 18

Setting up web-based administration 19
- Browser settings: 19

Logging on to Enterprise Edge 20

Logging off Enterprise Edge 21

Powering down the Enterprise Edge server 21

Rebooting the Enterprise Edge server 21

IP Routing 22
- IP Routing Overview 22
- Enterprise Edge IP routing specifics 23
- IP Addressing Overview 23
- Static Routing 24
- Routing Information Protocol (RIP) 24
- Enabling RIP on Network Interfaces 24
- Packet Filtering 24
- LAN-to-LAN Fast Path Routing 25

Dynamic Host Configuration Protocol (DHCP) 25
- Automatic Configuration using a DHCP server 26
- Guidelines for Using DHCP 26

Domain Name Service (DNS) 27
- Guidelines for Using DNS 27

Web Caching/Proxy 28
- Guidelines for Using Web Caching/Proxy 28

Simple Network Management Protocol (SNMP) 29
SNMP Overview 29
Guidelines for Using SNMP 29
Quality of Service 30
QoS overview 30
DiffServ Networks 31
Legacy Network 31
Admission Control 32
Packet Marking for DiffServ Networks 33
Port Range Setting for Legacy Networks 35
Relationship between the QoS Module and the VoIP QoS Monitor 36
Enterprise Edge QoS Restrictions and Defaults 36
LAN Connections 37
WAN Connections 37
WAN overview 37
Permanent WAN Connections 38
Frame Relay 38
PPP 38
Backup Up WAN Connection 39
Backup WAN Links 40

Chapter 4 Configuring Unified Manager Settings 41

Accessing system, resources, services and management settings on Unified Manager 42
Configuring system settings 42
System name 43
System performance graphs and tables 46
System Fault Alarm Banner 47
System name, date and time 49

Chapter 5 Configuring Resources Settings 51

LAN 52
WAN primary links 56
WAN Primary Link Summary Parameters 58
WAN Primary Link Line Parameters 59
WAN Primary Link Frame Relay Parameters 61
WAN Primary Link PPP parameters 65
WAN Primary Link performance graphs and tables 66
WAN Backup Links 67
WAN Backup Link Summary Parameters 68
WAN Backup Link Parameters 69
WAN Backup Access Parameters 71
MSC 72
Telephony 73

Chapter 6 Configuring Services Settings 75

DHCP 76
DHCP LAN 78
DNS 84
Routing 85
LAN Routing 86
WAN Routing 99
SNMP 101
SNMP Community List, Manager List, and Trap Community List 103
QoS 108
QoS performance graphs and tables 112
QoS filters 113
QoS Port Ranges 116
VoIP gateway 118
VoIP local and remote gateways 119
QoS monitor 124
QoS Monitor Mean Opinion Score 125
Web cache 126
NetLink Manager 127
Voice Record 129
Voice Record report settings 130
Voice Record report options 132
Voice Record market parameters 134
Voice Record PreFix 136
Voice Record Access/Suppress 137
TAPI Service Provider 138
Voice Service 140
Alarm Service 142
Voice Mail 143

Chapter 7 Configuring Management Settings 145

Configuring Management Settings 145
User Manager 145
Alarm Manager 148

Chapter 8 Diagnostics and Utilities 151

Saving System Settings 151
Downloading System Settings 152
Graphs and tables 154
Generating Statistics 154
Sample Rate 155
Error Messages 156
User Actions 156
Errors List 156

MIB II Information 161
Counters Shown at LAN and WAN Interface Levels 161
ICMP Counters 162
UDP Counters 163
TCP Counters 163
QoS Session Counters 163
QoS Best Effort Traffic Counters 163
QoS Dropped Packets Counter 164
QoS Graph Counters 164
QoS Best Effort Queue Counters 164

Appendix A: Troubleshooting 165

How to Get Help 165
Troubleshooting 165

Appendix B: Setting Up Remote Routers 167

Creating an Outbound Traffic Filter 167
Sample Criteria, Ranges, and Actions for UDP Filtering 168

Glossary 169

Index 177

Introducing Enterprise Edge 1

Routing and IP Services

Enterprise Edge supports the following routing and IP Services:

- Routing Services
  - IP Routing Protocol
  - RAS Service and Dial In Capabilities for Management Purposes Only
  - RIP
  - Packet Filtering
- IP Services:
  - DHCP
  - DNS
  - Web Caching
- VoIP (voice over IP) Service

  VoIP is a term used in IP telephony for a set of facilities that manage voice information delivery using Internet Protocol (IP). VoIP sends voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids ordinary telephone service tolls.

  VoIP derives from the VoIP Forum which promotes the use of ITU-T H.323 as the standard for sending voice (audio) and video using IP on the public Internet and within intranets. The VoIP Forum also promotes the use of directory service standards so that users can locate other users and the use of touch-tone signals for automatic call distribution and voice mail.

  In addition, VoIP uses the real-time protocol (RTP) over IP to help ensure that packets get delivered in a timely way. Using public networks, it is currently difficult to guarantee Quality of Service (QoS). Better service is possible with private networks managed by an enterprise or by an Internet telephony service provider (ITSP).

  When using VoIP a business positions Enterprise Edge as a gateway. The gateway receives packetized voice transmissions from users within the company and then routes them to other parts of its intranet (local area or wide area network) or sends them over the public switched telephone network.

System Software

Enterprise Edge provides services to end-users in a small office environment. The following services are managed through Enterprise Edge Unified Manager, a web-based user interface:

- IP Services
- VoIP Service
- Telephony Functions:
  - PBX Call Processing
  - Voice Mail
  - Call Center Solution with Auto-Attendant
- Management Server Module
- QoS Module

Using Enterprise Edge Unified Manager 2

This chapter introduces the major elements on the Enterprise Edge Unified Manager graphical user interface including navigation and menu descriptions.

Unified Manager lets you view and change configuration settings for:

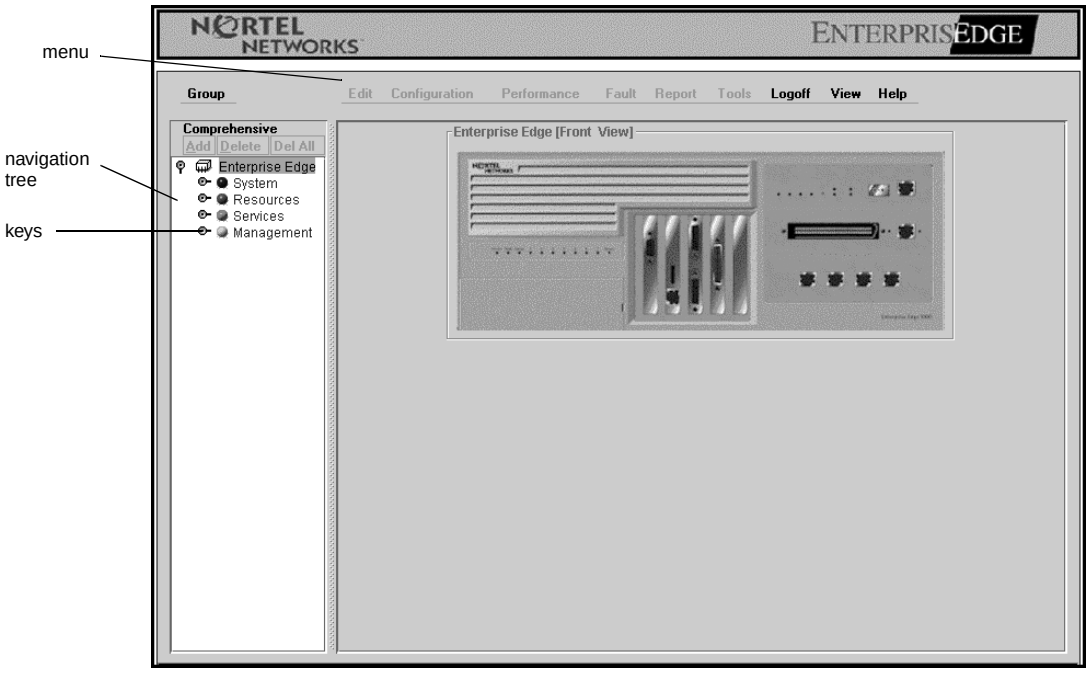
- IP Services
- VoIP Service
- Telephony Functions
- Management Server Module
- QoS Module

Understanding Unified Manager

The Unified Manager main view shows the Unified Manager view including:

- The menu where users click commands
- The navigation tree used for navigating between views and configuration screens
- The information panel view.

Unified Manager main view



As you navigate the menu tree shown in Unified Manager main view on page 9, Unified Manager displays configuration screens. The screens contain settings that you can edit to configure Enterprise Edge settings.

Enterprise Edge uses boxes and dialog boxes for configuring settings. Boxes let you to edit and save data line by line. Each time you tab to the next line, the previous line's values are saved. See Unified Manager main view on page 9 for an example.

If a value is invalid, a beep sounds and an error message appears to alert you of the error. The dialog box format allows you to enter text in boxes and save the settings by clicking the Save button. See Unified Manager main view on page 9 for an example.

The configuration screen contains:

- the title of the screen
- boxes
- scroll bars, when needed
- Save and Cancel buttons

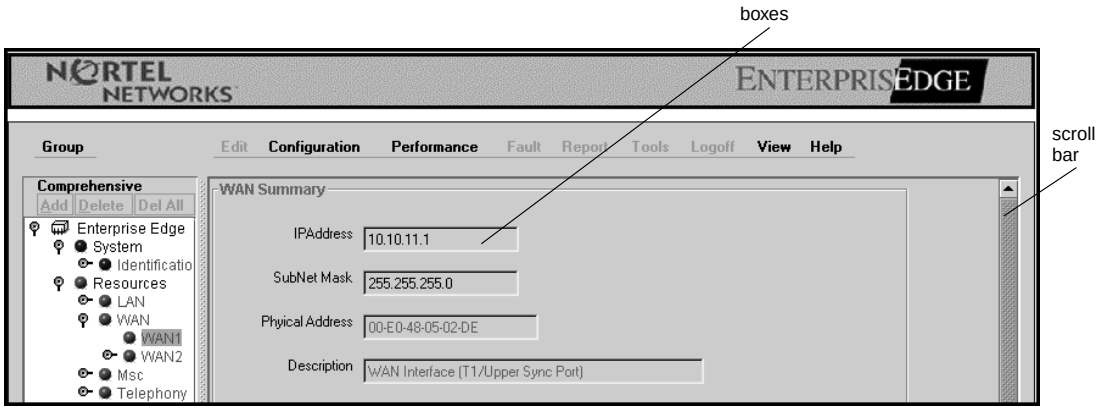
To configure settings:

1. Click keys on the navigation tree or click commands on the menu.
   The corresponding dialog box or screen appears.

2. Type the information in the appropriate box.

3. Click the **Save** button to save changes
   or
   click the **Cancel** button to close the configuration screen without saving any changes.

The following figure shows boxes and a scroll bar:



To make changes to boxes:

1. Click keys on the navigation tree until the configuration screen appears.
   See Unified Manager main view on page 9.

2. Type the updates in the appropriate boxes and follow the syntax that appears next to the box.
   If there is an error, a beep sounds and an error message appears.

3. Press the **Tab** key to move to the next box.
   Pressing the Tab key saves changes in the current box and moves the cursor to the next box..

Note: In some instances you must press the Tab key several times to move the cursor to the next box.

Changing the appearance of Unified Manager

You can choose from a Windows, Motif, or Metal look and feel.

To change the appearance of Unified Manager:

1. Click **View** and then click **Windows**, **Motif**, or **Metal.**
   The view changes to a Windows, Motif, or default Metal appearance.

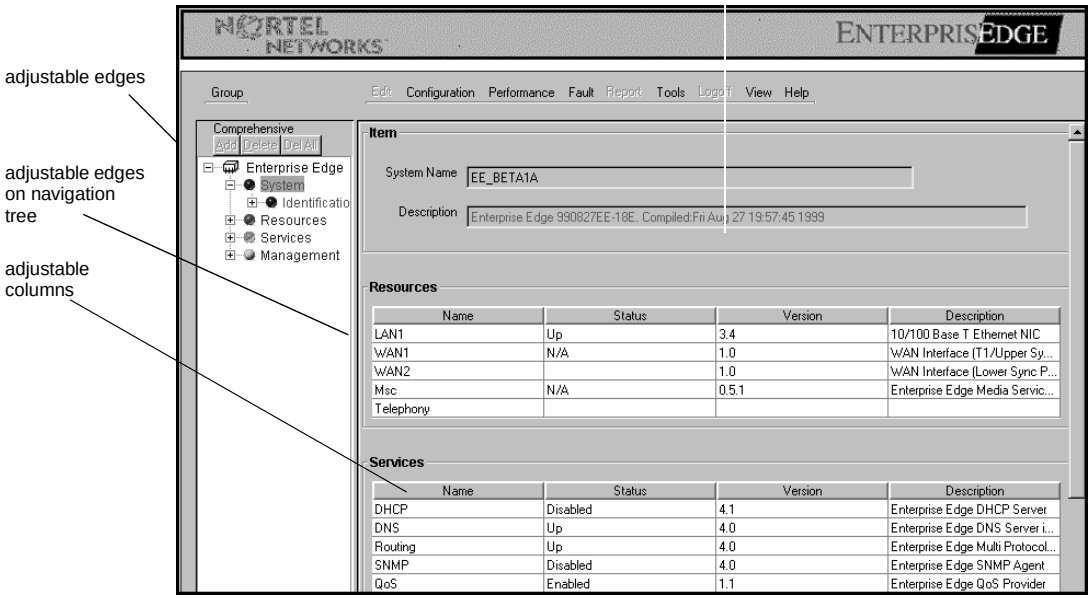
Adjusting Unified Manager views

The Enterprise Edge views are adjustable. You can resize Unified Manager and configuration screens.

To resize a view or screens:

1. Move the pointer over any edge until it changes to a double-headed arrow.

2. Drag the edge of the screen to the desired location and release the mouse.



Note: Each time you exit Unified Manager, the display returns to the default configuration.

Navigating between views

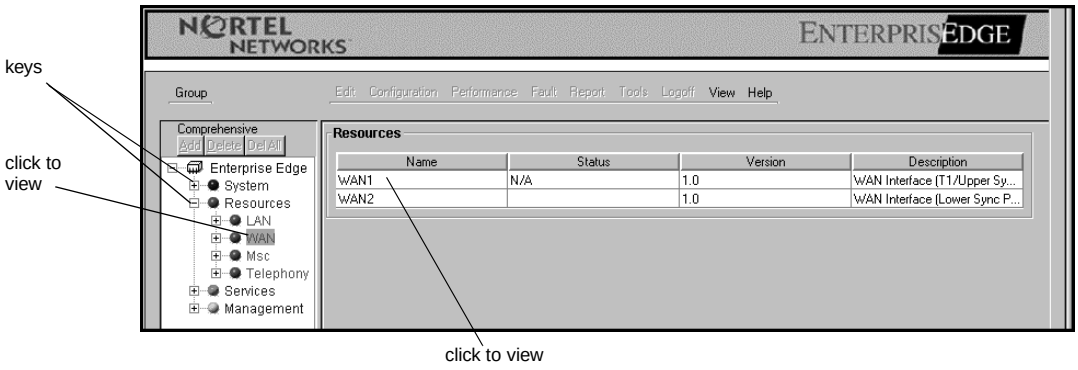
Choosing items in the navigation tree is the primary method for navigating the Unified Manager menu.

The navigate between views:

1. Point to an item in the navigation tree and click the key to expand to the desired view.

2. On the navigation tree, click the name of the item to display specific information.
   In this example, WAN is selected.

3. Click an item from the column to see information about it.
   In this example, WAN1 is selected.
   The resource information appears.



Changing column order

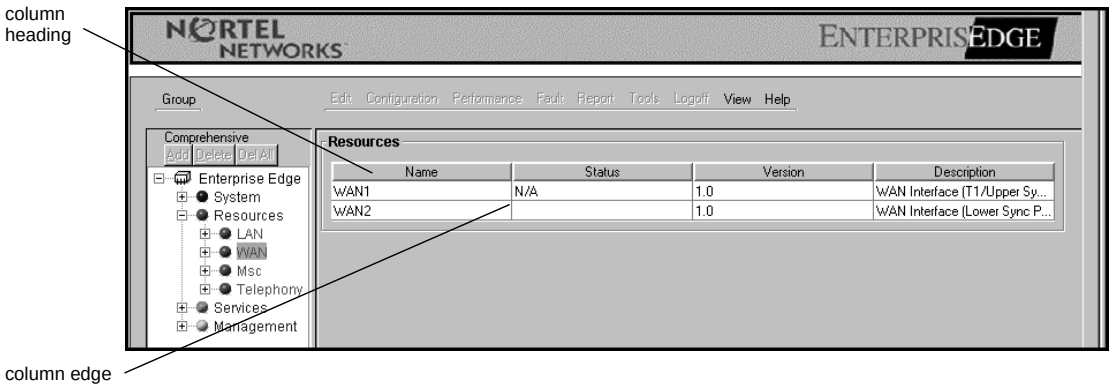
You can change the order and size of data views in Unified Manager. You can customize the view by resizing column widths or by reordering columns.

To change column order:

1. Click the column that you want to move.
2. Drag and drop the column to the appropriate location.

To change column width:

1. Move the pointer over any edge until it changes to a double-headed arrow.
2. Pull the column edge to the appropriate location.

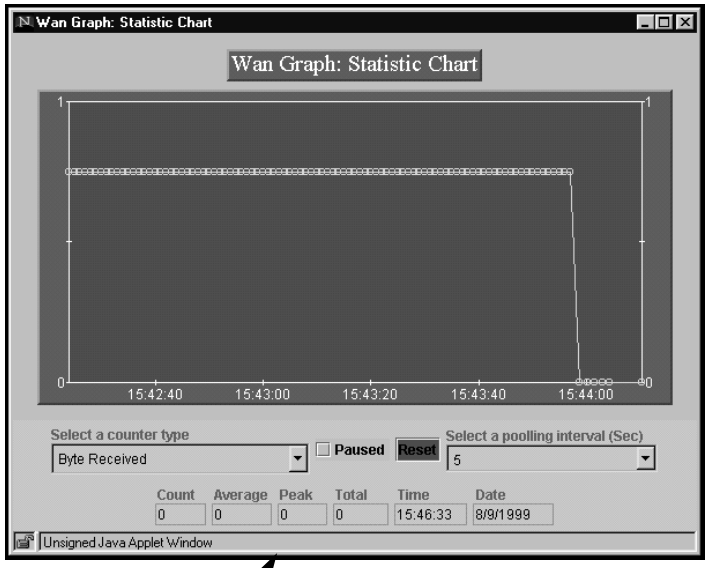


Generating statistics

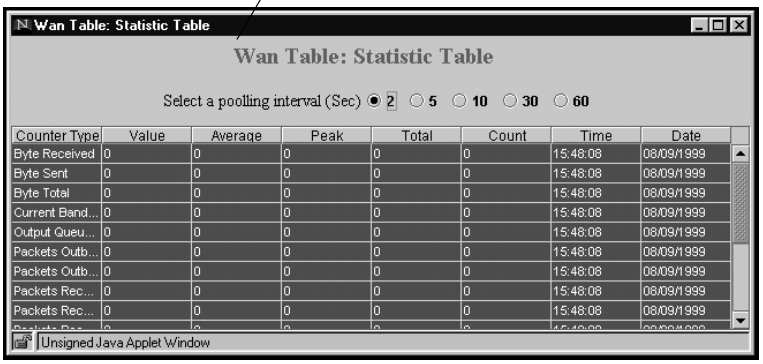
Enterprise Edge provides statistical information on Enterprise Edge server throughput and other performance-related information. The data is formatted in a Statistical chart or Statistical table format.

For additional performance information and instructions, see Graphs and tables on page 154.

Statistical chart



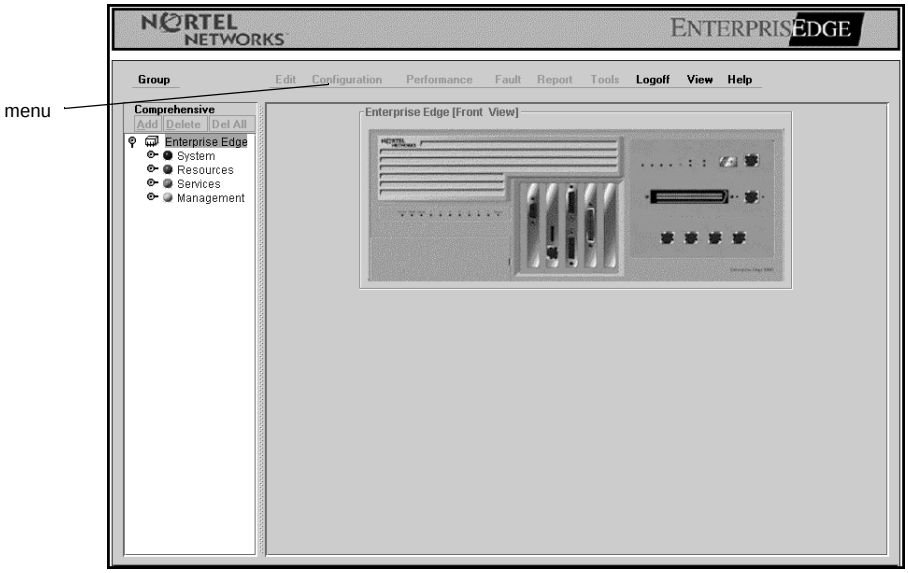
Statistical table



Menu descriptions

You access Enterprise Edge functions using the menu. The menu is dynamic which means that the menu commands change depending on the action a user takes.

Enterprise Edge menu



Menu descriptions

Use	To
Group	View the system, resources, services, and management.
Edit	Edit parameters.
Configuration	Access configuration dialog boxes and screens
Performance	Access performance graphs and tables.
Fault	Access fault management settings.
Report	Generate a report.
Tools	Use Enterprise Edge tools.
Logoff	Log off the Enterprise Edge server.
View	Change the appearance from Windows, Motif or Sun Swing.
Help	Access online help.

Using Enterprise Edge Services 3

This chapter includes information on:

- Enterprise Edge required parameters
- Setting up an Enterprise Edge IP Address
- Setting up web-based administration
- Logging on to Enterprise Edge
- Logging off Enterprise Edge
- Powering down the Enterprise Edge server
- Rebooting the Enterprise Edge server
- IP routing
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name Server (DNS) Service
- Web Caching/Proxy
- Simple Network Management Protocol (SNMP)
- Quality of Service (QoS)
- Using Traffic Filters
- Using Protocol Prioritization Queues
- LAN Connections
- WAN Connections

Enterprise Edge required parameters

The Enterprise Edge quick start module provides quick access to the parameters necessary for the Enterprise Edge server to become active online. However, you need to enter a minimum set of parameters within the quick start module. For more information, see the *Enterprise Edge Installation Guide*.

Obtain the required parameter values from an Internet Service Provider (ISP) or corporate network administrator.

Note: Nortel Networks recommends that after you powered on the Enterprise Edge server and connect with either an RS-232 or an Ethernet port, configure all the required parameters at the same time. After you configure the parameters, reboot the Enterprise Edge server from either the console or the graphical user interface (GUI).

Users must enter the following parameters:

- Initial IP and mask for all network interfaces
- Primary (and optional secondary) DNS servers
- Default next hop router
- Fractional T1 channel numbers (if you are using fractional TI)
- System name
- WAN Link Protocol
- Frame Relay DLCI / CIR (if applicable)
- V.90 modem dial-up username and password (if applicable)
- V.90 modem dial-up phone number and optional alternate phone number (if applicable)

The following table describes the Enterprise Edge server connectivity options.

Field	Definition
HTTP	You can launch your JAVA-enabled browser to connect to the Enterprise Edge server IP address that connects to your PC. This displays the log in screen. See the Enterprise Edge log on screen on page 20.
TTY	You can connect a dumb terminal to the console of the Enterprise Edge server through an RS-232 cross-over cable, or, you can use Hyperterminal from Win95/ Win NT systems. Refer to the installation guide for console menus.

Setting up an Enterprise Edge IP Address

To manage the Enterprise Edge server using a web browser or a Telnet connection, you must first set up the IP address. The Enterprise Edge server LAN interface is shipped with default IP 10.10.10.1 and mask 255.255.255.0.

To set up the Enterprise Edge server initial IP address using a RS-232 port:

1. Turn on the Enterprise Edge server power switch.
2. Connect a PC or laptop computer to the Enterprise Edge server RS-232 port.
3. Start a hyper terminal on the PC or laptop computer.
4. Enter the LAN/WAN IP address and other parameters.

To set up the Enterprise Edge server IP address using a LAN:

1. Turn on the Enterprise Edge server power switch.

2. Connect a laptop to the Enterprise Edge server by Ethernet (back-to-back by using a crossover cable to avoid disturbing the corporate LAN).

3. Set your PC or laptop computer IP address to 10.10.10.2 with a mask 255.255.255.0.

4. Start a web browser on your laptop with a URL 10.10.10.1.

Setting up web-based administration

To establish web-based administration, a workstation needs to be set up as an Enterprise Edge client with Internet Explorer 4.0 or greater and a JAVA Virtual Machine (JVM) 5.0.0.2922 or greater installed.

To install JVM on a workstation, search the Microsoft information web page for instructions.

This minimum PC requirements are discussed in Enterprise Edge specifications.

Note: The ideal display for a monitor attached to Enterprise Edge is 1280 x 1024.

Browser settings:

Set your browser as follows:

Program	Required Settings
Netscape Communicator 4.5 or greater	Click Settings: Edit: Preferences Category Advanced set Enable Java: On set Category: Cache set Cached document comparison: Every Time
Internet Explorer 4.0 or greater	Choose Views: Internet Options Category: General: Temporary Internet Files: Settings click Check for newer versions of stored pages: Every visit to the page set Advanced Java VM set Java JIT compiler enabled

Enterprise Edge OA&M allows multiple users to log on. If each user that logs on attempts to configure the same or related subsystems, the most recent modification remains in effect and overwrites changes by another administrator. Administrators must be careful to not make any unintended changes.

Nortel Networks recommends that only one administrator user account is maintained in Enterprise Edge and access is closely controlled. Administrators must coordinate changes to avoid unintended changes.

Note: Do not use proxy servers while configuring Enterprise Edge using WEB OA&M. You must disable proxies and directly access Enterprise Edge. The configuration procedures depend on the browser and version.

Logging on to Enterprise Edge

To log on to Enterprise Edge:

1. Open a web browser.

2. In the address, type the Enterprise Edge IP Address in a web browser.
   For example: HTTP://10.10.10.1

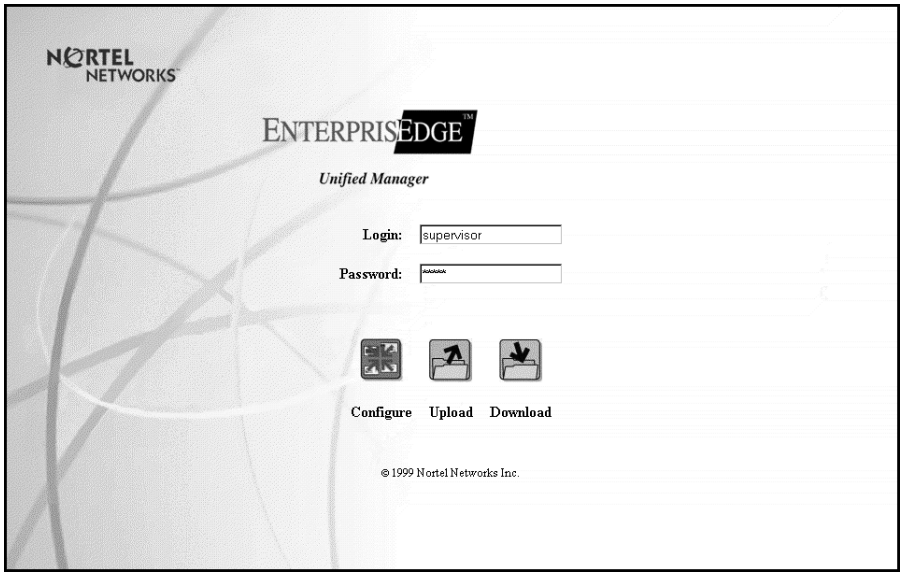
3. Press the **Enter** key.
   The Enterprise Edge log on screen appears

4. In the **Login** box, type your log on name.
   The default log on name is *supervisor*.

5. In the **Password** box, type your password.
   The default password is *super*.

6. Click the **Configure** button.
   The Enterprise Edge Unified Manager software starts. Consult your system administrator for appropriate information. Depending on your system, Unified Manager software can take up to several minutes to initialize.

Enterprise Edge log on screen



The log on screen includes these boxes:

Field	Definition
Login	The user name. The name can contain up to 50 case-sensitive alphanumeric characters. The default log in name is s*upervisor*.
Password	The Enterprise Edge password. The password name can contain up to 12 case-sensitive alphanumeric characters. The default password is *super*.
Configure	lets you access Enterprise Edge configuration.
Upload	lets you upload and apply Enterprise Edge settings and system settings.
Download	lets you download and save Enterprise Edge settings and system settings.

Logging off Enterprise Edge

To log off Enterprise Edge:

1. Click the **MSP** icon on the left frame.

2. On the menu click **Logoff** and then click **Logoff**.
   A message appears that asks you to confirm your request to log off.

3. Click the **Yes** button to log off.

Powering down the Enterprise Edge server

To power down the Enterprise Edge server:

1. From the menu of the console, quit Enterprise Edge.

2. Remove the power connection.

Rebooting the Enterprise Edge server

To reboot the Enterprise Edge server:

1. Click **Logoff** and then click **Reboot**.
   A message appears that asks you to confirm your request to reboot.

2. Click the **Yes** button to reboot.

IP Routing

This section includes information on:

- IP Routing Overview
- Enterprise Edge IP routing specifics
- IP addressing overview
- Static routing
- Routing Information Protocol (RIP)
- Packet Filtering
  - source address
  - destination address
  - IP Protocol ID
  - TCP Port
  - UDP Port
  - ICMP Type
  - ICMP Code
- LAN to WAN routing
  - managing traffic using Interrupt Modulation
- LAN to LAN routing
  - Fast Path Routing

IP Routing Overview

The Internet Protocol (IP) is the protocol used on the Internet to send data is sent from one computer to another. Each computer on the Internet, called a "host", has at least one address that identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail or a web page), the message gets divided into units called packets. Each of these packets contains both the sender's Internet address and the receiver's Internet address.

A packet is first sent to a router that understands reads the destination address and forwards the packet to an adjacent router that reads the destination address.This routing process continues across the Internet until one router recognizes the packet as belonging to a computer in its immediate neighborhood or domain. That router forwards the packet to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than the order they are sent. Another protocol, the Transmission Control Protocol (TCP) to put the packets in the right order.

IP is a connectionless protocol, which means that there is no established connection between the end points that communicate. Each packet that travels through the Internet is treated as an independent unit of data without any relation to another unit of data. The packets get put in the right order because TCP, the connection-oriented protocol, keeps track of the packet sequence in a message. In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

Enterprise Edge IP routing specifics

Using Enterprise Edge Unified Manager, you can perform the following routing configuration options:

- Add or delete the interfaces to routing protocols
- Configure routing protocol options
- Add and delete static routes
- Add or delete filters
- Set filter actions

For instructions on configuring routing options, see Routing on page 85.

The followings table shows the Enterprise Edge IP routing protocols and the precedence order when conflict or redundant routes occur.

Precedence	IP Routing Protocols
1.	Static Routing
2.	SNMP
3.	RIP v1 and v2

IP Addressing Overview

IP addresses follow the format nnn.nnn.nnn.nnn, where nn is a number between 0 and 255. For example, 192.123.4.56 or 10.1.1.1. IP addresses enable computers to communicate to each other. Both servers and workstations on a network must have IP addresses. There are two types of IP addresses:

Dynamic – A dynamic IP address changes. Dynamic IP addresses are assigned to computers by an IP address server as the computer needs it. Usually there is a particular range or scope of IP addresses that your network uses. With dynamic IP addressing, a computer can have a different IP address every time it connects to the network. Other devices need to know the computer's IP address so that they can communicate with it. The IP address server manages the assignment of IP addresses to the client workstations.

Static – A static or fixed IP address never changes. It is assigned to a computer permanently. The computer has the same IP address every time it connects to the network and is known to other devices on the network by that IP address.

Static Routing

Enterprise Edge users can add static routes to the IP routing table. These static routes take precedence over those routes chosen by routing protocols, such as RIP.

To add a static route, see Static Route on page 94.

Note: Ensure that users do not add a static route for default route 0.0.0.0 with mask 0.0.0.0. Enterprise Edge's Net Link Manager automatically creates a default route and adjusts it according to link status unless router or Net Link Manager are running.

Routing Information Protocol (RIP)

RIP is a widely-used protocol for managing routing information in a self-contained network such as a corporate intranet. RIP is classified by the Internet Engineering Task Force (IETF) as one of several internal gateway protocols (IGPs).

A RIP router sends full updates, which list all the other hosts it knows about, to its closest neighbor host every 30 seconds. The neighbor host sends the information to its next neighbor, until all the hosts in the network know the routing paths, a state known as network convergence. RIP uses a hop count to determine network distance. Each host with a router in the network uses the routing table information to determine the next host for the packet, until a specified destination is reached.

Enabling RIP on Network Interfaces

To run RIP on one or more network interfaces, go to the specific interface under router and enable RIP. After you enable RIP for an interface, you do not have to reboot the Enterprise Edge server for the changes to take effect.

Packet Filtering

A packet is a unit of data routed between an origin and a destination on the Internet or on any other packet-switched network. When any file such as an e-mail message, HTML file, GIF file or URL request, is sent on the Internet, the IP layer divides the file into packets of an efficient size for routing. Each of these packets is numbered and includes the Internet address of the destination.

Enterprise Edge supports basic (or stateless) packet filtering for IP. You can configure the filter to pass only the packets from the routes they list, or to pass everything except the packets for the routes they list.

Each route in the list can be any combination of the following packet filtering features. By default, no packet filer is configured.

Enterprise Edge supports the following packet filtering features for IP:

Packet Filter Feature	Comments
Source Address	the source address field of the packet to be filtered.
Source Mask	the source address mask of the packet to be filtered.
Destination Address	the destination address field of the packet to be filtered.
Destination Mask	the destination address mask of the packet to be filtered.
Protocol	the protocol type of the packet to be filtered.
Source Port	the source port of the packet to be filtered. This field applies only if protocol value is TCP or UDP.
Destination Port	the destination port of the packet to be filtered. This field applies only if protocol value is TCP or UDP.
ICMP Type	the ICMP type field of the packet to be filtered. This field applies only if protocol value is ICMP.
ICMP Code	the ICMP type field of the packet to be filtered. This field applies only if protocol value is ICMP.

Note: When you set filters, you must forward packets going to the RPC port (port 135 TCP or UDP) for correct Unified Manager operation.

LAN-to-LAN Fast Path Routing

Enterprise Edge provides an optional second 10/100 LAN interface. If the second LAN interface is used, Enterprise Edge uses optimized software for high performance routing. This includes an innovative design that speeds up the performance for LAN-to-LAN routing by over three times the rate that is normally achieved using traditional software architecture.

Dynamic Host Configuration Protocol (DHCP)

DHCP (Dynamic Host Configuration Protocol) is a protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. If an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.

Without DHCP, the IP address must be entered manually at each computer. If computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address if a computer connects to a different place in the network.

You can set up Enterprise Edge to be your LAN’s DHCP server and let it assign IP addresses to the workstations on your LAN as they need them. This is the recommended configuration.

If you set up the Enterprise Edge server as a DHCP server, you must let all of your workstations know that they will have their new IP addresses assigned by Enterprise Edge. To do this, you may need to change the configuration of each workstation individually.

If you already have a DHCP server, you must let it know that the Enterprise Edge server is their gateway and DNS proxy for the workstations.

Your Enterprise Edge server can function as a DHCP server. You can use this feature if you do not want to administer static IP addresses for every workstation on your network. You can configure Enterprise Edge to assign IP addresses dynamically.

Automatic Configuration using a DHCP server

To configure the DHCP server, you need to create a particular range (or scope) for each LAN interface in Enterprise Edge and allocate a block of IP addresses for that scope. The Enterprise Edge Auto-Configure system automatically creates a scope using parameters inherited from the LAN interface.

Guidelines for Using DHCP

Since many default DHCP parameters are inherited from LAN interface parameters, configure LAN interfaces before configuring DHCP.

If you are modifying the DHCP configuration on Enterprise Edge, follow the same guidelines of your organization. In particular, you can perform one or more of the tasks listed below to ensure proper operation of the networked system:

1. If a change in the DHCP configuration resulted in the change of ‘Router’ and ‘Subnet mask’ options in a scope, users must do one of the following to ensure basic operation:
   - Execute ipconfig /release and ipconfig /renew on each of the workstations. For Windows 95 and Windows 98, use its equivalent, winipcfg.
   - For clients that do not support ipconfig and winipcfg, reboot is required to renew their IP addresses.
2. If change in DNS server or DNS name options happens, users need to repeat the tasks in step 1 to ensure proper connectivity with the organization.
3. Always schedule a down time associated with these changes.
4. Nortel Networks recommends that you reboot Enterprise Edge to initialize changes.

Using Enterprise Edge, you can define a DHCP scope for each LAN interface. DHCP server parameters are divided into two categories: global and scope specific. Global parameters apply to all scopes. Specific parameters apply to a specific scope.

Domain Name Service (DNS)

The domain name service (DNS) is the system within the Internet that maps names of objects, usually host names, into IP numbers or other resource record values. The name space of the Internet is divided into domains. The responsibility for managing names in each domain is usually delegated to systems in each domain.

Enterprise Edge functions as both a gateway to the Internet and as a DNS proxy:

- **Gateway**: a system that links two different types of networks and enables them to communicate with each other. Enterprise Edge is the gateway that links your company's network to the Intranet or Internet. Depending on your configuration, you can let your workstations know that Enterprise Edge is your Internet gateway.

  Note: If your PC is a DHCP client under Enterprise Edge, you do not have to do this.

- **DNS Proxy** – A Domain Name Service (DNS) proxy translates alphabetic domain names into computer-readable IP addresses. For example, the domain name www.nortelnetworks.com for the Nortel Networks web site can translate to the IP address 192.177.5.18. After a domain name is translated into an IP address, the workstations on your network can communicate with the web site. Depending on the configuration of your system, you can let your workstations know that Enterprise Edge is the DNS proxy.

When Enterprise Edge receives DNS requests from clients, it first checks its local cache for name entries and records. If found locally, Enterprise Edge immediately responds to clients. Otherwise, Enterprise Edge creates a new DNS request to the remote Primary or Secondary DNS servers on behalf of the client. If the remote DNS server responds with the requested records, they are forwarded to clients and cached in Enterprise Edge.

Note: If your PC is a DHCP client under Enterprise Edge, you do not have to let your workstations know that Enterprise Edge is your DNS server.

Guidelines for Using DNS

Consider the following guidelines when using DNS:

- If the Enterprise Edge DNS service is enabled, make sure that clients always use Enterprise Edge as their DNS server.
- When it is disabled, set the DNS Server field in DHCP configuration to the remote DNS server IP address. If DHCP service is also disabled in Enterprise Edge, tell all clients to set the DNS server in their IP configuration to the remote DNS server.
- The DNS proxy carries security features because it keeps all of the internal IP addresses from external web servers.
- You are required to fill in the remote Primary DNS server IP address. See DNS on page 84 for instructions.

Web Caching/Proxy

When you use Enterprise Edge as a web proxy, Enterprise Edge can store or cache information downloaded from the Internet. A proxy is a server that acts on behalf of another. Web caching allows LAN workstations to share common information downloaded from the Internet.

Data is usually cached on individual workstations. Each time a workstation on the LAN requests information from the Internet, the individual's request is sent to the Internet, and the information is returned to their workstation. If multiple LAN workstations request common data, a web cache on the network reduces download time from the Internet.

With Enterprise Edge configured as a web proxy with web caching:

- LAN workstations have shorter download times.
- Previously downloaded information is stored for future use by all workstations on the LAN.
- Enterprise Edge retrieves information from the Internet only if it is not already cached or if the cached file is out of date compared to the information on the Internet.
- Cookie blocking protects users' privacy.

You can configure the web caching settings through your web browser.

The web proxy also provides security features similarly to the DNS proxy because it hides all of the internal browsers' IP addresses from external web servers. External web servers see Enterprise Edge's IP address.

Guidelines for Using Web Caching/Proxy

The Enterprise Edge web proxy uses a web server for running in HTTP-Proxy mode.

Consider the following guidelines when using web caching/proxy:

- A web server installed in Enterprise Edge can not be used as a general purpose HTTP server. It is only used by the Enterprise Edge web-based management client and web-cache services.
- If users need to run their web sites, they need to run the HTTP Server on another system and make its IP address known to Enterprise Edge.

To set the web server as the web cache/proxy, refer to Web cache on page 126.

Simple Network Management Protocol (SNMP)

This section includes information on:

- SNMP Overview
- Guideline for Using SNMP

SNMP Overview

Simple Network Management Protocol (SNMP) is the protocol that governs network management and the monitoring of network devices and their functions.

Guidelines for Using SNMP

Consider the following guidelines when using SNMP:

- You can set read-only and read-write community names.
- You can set a list of permitted managers. When set, the agent responds to requests from SNMP managers from only those IP hosts.
- An empty list of permitted managers implies that agent responds to requests from anyone.
- You can set trap communities. Each trap entry identifies the community name that must be used and the manager addresses.
- You can enable or disable sending authentication traps.
- You can enable or disable the SNMP agent.
- At present, SNMP supports only MIB-II (RFC 1213) MIBs.

Quality of Service

This section includes information on:

- QoS overview
- DiffServ networks
- Legacy networks
- Admission control
- Packet marking for DiffServ networks
- Port range setting for legacy networks
- Relationship between the QoS Module and the VoIP QoS monitor
- Enterprise Edge QoS restrictions and defaults

QoS overview

On the Internet, Quality of Service (QoS) is the methodology that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of concern for the continuous transmission of high-bandwidth voice and video multimedia information. Transmitting this content dependably is difficult in public networks using ordinary “best effort” protocols.

Real-time applications that include voice and video are time-sensitive. Delivering voice and video over the Internet requires bounded packet delay and jitter. Differentiated Services (DiffServ) is a QoS framework standardized by IETF that focuses on DiffServ standards for real-time and mission critical applications. The DiffServ standards are evolving and vendors are starting to develop network devices that support DiffServ.

The purpose of the Enterprise Edge QoS module is to prioritize IP traffic and to provide an acceptable quality of service to delay and jitter sensitive applications such as audio and video as well as mission critical applications.

The Enterprise Edge QoS module primarily serves two purposes:

- In a DiffServ network, it acts as an edge device and performs the packet classification, marking, and prioritization.
- In a non-DiffServ or legacy network, it manages the WAN link to make sure premium voice (and optional video) packets get high priority when crossing the slow WAN link in both directions.

DiffServ Networks

For DiffServ networks, Enterprise Edge:

- Intercepts all H.323 traffic
- Identifies call setup packet
- Performs admission control based on the WAN link usage
- Marks the packets as premium once admitted

Enterprise Edge implements the DiffServ queuing model that includes a premium queue and eight best-effort queues. The premium queue has a stricter high priority than the best-effort queues. The eight best-effort queues are scheduled by a weighted-fair-queuing (WFQ) algorithm. Since best-effort traffic is not shaped and does not go through the admission control process, the WFQ is needed to avoid starvation of low priority packets.

Currently, H.323 traffic is allowed to get into the premium queue. Users can allow other traffic to be premium by setting up priority filters on the web-based GUI using the following filter criteria:

- Source IP address (with mask)
- Destination IP address (with mask)
- IP protocol ID (e.g. TCP, UDP, or ICMP)
- Source port range
- Destination port range
- Incoming TOS field

Note: There is no traffic shaping mechanism implemented in this version. Be cautious when setting up premium priority filters. If the traffic is high volume and with high bursts, it may impact VoIP quality. Unless necessary, Nortel Networks recommends that you allocate traffic to the high priority best-effort queues instead of the premium queue.

Legacy Network

In a legacy network, Enterprise Edge assumes that network devices, such as routers and switches, do not recognize the IP header TOS field (as defined by DiffServ) and do not perform the corresponding priority processing. However, most of the current installed routers, including those from Cisco and Nortel Networks, allow administrators to set up priorities by IP addresses, port numbers or protocol types, which is similar to the priority filters described above.

Note: This information is specific to H.323 traffic in legacy networks.

In this environment, Enterprise Edge allows H.323 voice (and optional video) packets to travel across the WAN link with high priority in both directions using existing router features.

An administrator needs to reserve a block of UDP port numbers and configure them as high priority in both Enterprise Edge and the remote router at the other end of the WAN link. Enterprise Edge forces all of the admitted H.323 streams to fall into the reserved port range by using a proprietary technique so that these H.323 voice (video) packets can get high priority. This is completely transparent to the end H.323 terminals.

See Appendix B: Setting Up Remote Routers on page 167 for additional information on setting UDP port ranges for remote routers.

Note: If an administrator configures all routers in their corporate network with the same reserved port numbers (both in and out), admitted H.323 streams can get end-to-end high priority. However, routers connected to WAN links are more critical because they are typically the bottlenecks.

You can set up best-effort traffic priorities through the web-based Unified Manager by using the following filter criteria:

- Source IP address (with mask)
- Destination IP address (with mask)
- IP protocol ID (e.g. TCP, UDP, or ICMP)
- Source port range
- Destination port range
- Incoming TOS field

There are a total of 8 priority classes for best-effort traffic in Enterprise Edge. By default, all best-effort traffic is sent to Class 5 (queue 5), with Class 1 the highest and Class 8 the lowest in priority.

Admission Control

Enterprise Edge allows users to set a certain percentage of the WAN bandwidth for premium traffic. This traffic takes strict priority over best-effort traffic. In this version, H.323 (VoIP) flows need to pass the admission control process to be treated as premium traffic.

For admission control, Enterprise Edge uses the WAN Premium Bandwidth parameter. Specifically, for each H.323 flow, QoS performs admission control using the negotiated coding algorithm. A flow is admitted as a premium flow if the current total WAN premium usage plus the new flow is lower than the allocated WAN premium bandwidth.

Otherwise, the flow is rejected and he flow is still delivered as best-effort traffic.

As a reference point: for a typical G.729 codec, each VoIP flow requires the following WAN bandwidth, depending on the codec sample rate:

G.729	Sample Rate 30 ms	Sample Rate 20 ms	Sample Rate 10 ms
No Compression	10.6 k	14 k	24 k
Data Compression	8 k	10 k	16 k
RTP Hdr Comp.	5.8 k	6.8 k	9.6 k

Note: The calculation is based on a full-duplex WAN link with HDLC overhead and VoIP with silence suppression.

Nortel Networks recommends that for slow WAN links, such as a 56K leased line or ISDN, H.323 video is not configured as premium traffic.

Packet Marking for DiffServ Networks

Enterprise Edge classifies traffic and marks packets by setting the IP header type of service (TOS) field. By default, the following items are classified as premium traffic:

- All VoIP flows
- RIP packets: routing packets are periodically exchanged between Enterprise Edge and remote routers. These packets need higher priority than regular packets to ensure that the routing protocol is working properly.
- ICMP packets: Enterprise Edge Net Link Manager uses the ‘ping’ command to decide whether the primary WAN link is active or inactive. These packets are not delayed by regular packets.
- UDP Port 5000 packets – Enterprise Edge VoIP QoS Monitor uses port 5000 in a proprietary protocol to monitor the IP network delay and jitter. Since Enterprise Edge assigns VoIP packets to the premium queue, it also gives these monitor packets high traveling priority.
- Admitted RTP/RTCP packets.

In Enterprise Edge, there are two places a user can set up a TOS field in an IP header:

TOS-for-Premium-Traffic – this field sets TOS bits for premium packets for DiffServ networks. If this field is ignored, Enterprise Edge uses a default value of 0xB8.

TOS-for-Priority-Filters– this field sets TOS for those packets matching a specific priority filter.

Note: You can specify packets matched to a filter to go Priority Queue 0 – 8. The Queue 0 is for premium packets, and Queue 1 – 8 correspond to best-effort priority classes 1 – 8.

If you specify Queue 0 and a TOS bits for a filter, then this TOS takes precedence over the TOS set for premium traffic for all packets that match this filter.

The default TOS for all best-effort packets is 0x00, and the default queue for best-effort packets is Queue 5.

WARNING
Premium flows that are specified by priority are not admission controlled. Unless you know the behavioral characteristics of a flow, do not specify flows as premium. Instead, you can specify them as the highest B-E traffic.

Consider the following guidelines when you set up priority filters

- The fewer the conditions to check for, the fewer CPU cycles are consumed. Filter processing is faster if fewer conditions are specified, without compromising the precision in selection.
- If you don't need the value of a particular criterion, such as source port number, don't set a corresponding value for the filter.
- When you specify the layer 3 sub-protocols, use the port number/IP address combinations and avoid specifying the protocol field. Nortel Networks recommends that you specify a protocol field only if you manage an unusual condition in your network. This reduces the consumption of CPU cycles.
- Users can configure the precedence of the filters. Packets are matched against each filter sequentially until a match is found. Pay attention when specifying the precedence of filters. Placing 'popular' filters ahead of 'unpopular' filters can significantly speed up the processing.

Port Range Setting for Legacy Networks

Enterprise Edge uses UDP port ranges to provide high priority to VoIP packets in existing legacy IP networks. These same port ranges must be reserved and set to high priority on all routers that an administrator expects to have QoS support. Reserving port ranges is not required for DiffServ networks.

You can select any port ranges that are not used by well-known protocols or applications.

Each H.323 or VoIP RTP flow uses two ports. The total number of UDP port numbers to be reserved depends on how many concurrent RTP flows are expected to cross a router interface. In general:

- Backbone routers reserve more ports than edge routers.
- Edge routers' port ranges are a subset of the backbone router port ranges.
- Add UPP 5000 to high priority.
- Enterprise Edge's port ranges are a subset of the remote router's port ranges.
- You must reserve two ports for each voice call you expect to carry over the WAN. You need two ports for each video session if it is given premium treatment.
- You can reserve multiple discontinuous ranges. Nortel Networks requires each range meet the following conditions:

  - Each range must start with an even number.

  - There must be an even number of ports in a range.

See Appendix B: Setting Up Remote Routers on page 167 for additional information on setting UDP port ranges for remote routers.

Relationship between the QoS Module and the VoIP QoS Monitor

The VoIP gateway in Enterprise Edge includes a Quality-of-Service Monitor (QMON) that periodically monitors the delay and jitter of IP networks between two peer gateways by using a proprietary protocol. These monitoring packets are delivered at UDP port 5000.

The main objective of the QMON is to allow new VoIP calls to fall-back to PSTN if the IP network is detected as “bad”.

The QoS module discussed here complements QMON. While QMON passively monitors the IP network, the QoS module actively improves the IP network by giving VoIP packets higher priority to travel so that the chance for QMON to detect “bad” is reduced.

Note: For a VoIP call, if a packet passes QMON but fails the QoS admission control, it is delivered over IP but only as a best-effort flow. There is no fall back to PSTN if a packet has passes QMON checking.

QMON packets travel at the same priority as VoIP packets or at higher priority than normal IP packets. If VoIP packets travel at a premium level but QMON packets travel at normal best-effort level, it is possible for QMON to report the IP network as “bad” and start to PSTN fall-back, but the actual delay and jitter for VoIP packets are still “good”, since VoIP packets have a higher priority. To avoid this add UDP port 5000 to the high priority queue in all routers.

Enterprise Edge QoS Restrictions and Defaults

Enterprise Edge QoS includes the following restrictions and defaults:

- By default, the general bulk of traffic (not defined by priority filters) is routed to best-effort Queue 5 (with Queue 1 the highest priority and Queue 8 the lowest). An administrator can define four classes of traffic above the generic traffic and three classes below it.
- A maximum of 31 priority filters for best-effort traffic can be created.
- The QoS module can be optionally turned ON or OFF. The default setting is on.
- The predetermined WAN bandwidth is always available to VoIP gateway channels. That is, VoIP gateway calls are always admitted. The remaining WAN premium bandwidth can be used by other H.323 streams, such as Microsoft NetMeeting. If there is no VoIP gateway traffic, their WAN bandwidth can be used only by best-effort traffic, not other premium traffic (for example, Netmeeting). Enterprise Edge does not support preemption of admitted premium streams.
- Currently packet prioritizing and priority filters apply only to outbound traffic for specified interfaces. Inbound traffic is treated on a first in first out (FIFO) priority.
- The maximum port numbers a user can reserve for premium traffic is 256.

LAN Connections

The Enterprise Edge Ethernet / 802.3 interface supports IEEE 802.3 Ethernet frame format. The Ethernet interface uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to manage the access to the physical media.

Enterprise Edge Ethernet interface supports the following features:

- 100 BASE – TX with RJ-45 connector
- 10 / 100 Auto Sense
- Full Duplex support
- Fast LAN-LAN routing

WAN Connections

This section includes information on:

- WAN overview
- Permanent WAN connections:

  – Frame Relay

  – PPP

WAN overview

A WAN (wide area network) is a geographically dispersed data communication network. The term WAN distinguishes a broader data communication structure from a local area network (LAN). A WAN can be privately owned or rented, but usually connotes the inclusion of public (shared user) networks.

Enterprise Edge includes two primary WAN links (WAN1, WAN2) and a backup WAN dial up link (WAN3).

- The Primary WAN link is always a permanent link and it is a dedicated network adapter. The primary link runs either Frame Relay or the PPP protocol at the link layer.

  The Enterprise Edge primary WAN connection is through a two-port card. These two ports can be independently configured to run Frame Relay or PPP. The card includes one serial sync port and one T1 port.

- The backup WAN link is always configured as dial-on-demand network adapter by the router. The backup Wan link runs PPP only. Enterprise Edge provides backup WAN connection through a V.90 modem.

  The primary and backup link management is performed from Enterprise Edge. There is a Net Link Manager running in Enterprise Edge that monitors the primary link status and it starts the backup link when a break in primary link is detected. Similarly, the backup link is automatically terminated when the primary link becomes active.

Note: Net Link Manager can back up only one link, even though there are two primary links. Net Link Manager backs up the link whose next hop address is given to it.

- Net Link Manager manages the default route in Enterprise Edge. If a link breaks, Net Link Manager removes all the default routes on the broken link and adds the default route to the new link. This happens during switch over from primary to secondary links and vice versa.

Permanent WAN Connections

This section includes information on the following topics:

- Frame Relay
- PPP

The permanent WAN connections are provided by a WAN card that supports PPP and Frame Relay connections. Each port can be configured to run either of the protocols independently.

The WAN cards are provided by one T1 port (with in-built CSU/DSU) and one serial sync port or dual serial sync port versions.

The Enterprise Edge serial sync port supports the following:

- Interfaces: V.35, RS442, RS 323, X.21
- Maximum line speed:8 Mbit/sec

Frame Relay

Enterprise Edge supports Frame Relay in *group* mode. That is, for each physical port (serial sync or T1 port), there is one IP address for all PVCs.

The available DLCI numbers are 0-1023, of which 16 are reserved. The maximum number of PVC’s allowed is 1008.

For Frame Relay network, Enterprise Edge supports Frame Relay Forum standard FRF.9 compression protocol with the standard STAC compression algorithm.

Software performs the compression and it can be enabled or disabled by using Unified Manager.

PPP

Point-to-Point Protocol (PPP) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP). PPP is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP can process synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection.

PPP on the primary WAN link uses synchronous point-to-point communication. Because the physical media is point-to-point, authentication attributes are not supported in this mode.

Enterprise Edge supports PPP Compression Control Protocol (CCP) (RFC 1962) with STAC compression algorithm.

This compression is done by software and can be enabled or disabled by using a parameter in PPP configurations.

Backup Up WAN Connection

In Enterprise Edge, the back up WAN connection is a V.90 modem that is used as a dial-up WAN link.

The modem is provided through an RJ-11 connector. The modem has the following features:

- V.90 56 kbps ITU standard
- V.34 33.6 kbps ITU standard
- V.42/MNP 2-4 error control
- V.42 bis/MNP 5 data compression
- Compatible with ITU and Bell Standards from 56 kbps down to 1200 bps

Note: The modem is capable of receiving at up to 56 kbps and sending at up to 31.2 kbps. Because of FCC regulations, receiving speeds are limited to 53 kbps. The actual speed can vary, depending on factors such as current line noise.

Backup WAN Links

Enterprise Edge supports Microsoft Point-to-Point Compression (MPPC), RFC 2118 for traffic across dial-up links. The compression ratio of MPPC is approximately 4-5 to 1.

For the remote backup, Enterprise Edge supports the following authentication mechanisms:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP) is a more secure procedure for connecting to a system than the PAP. The system attempts CHAP before using PAP.

  Software data compression on backup/dial up link is an optional feature in Enterprise Edge. The default is set to ENABLE data compression.

Note: Remote user dial in as a RAS client is supported for administrative purposes only.

Guidelines for Using Remote Dial In

Consider the following guidelines when using remote dial in:

- The same modem is shared between the remote dial-in for administration and the backup WAN link. If a remote administration user is connected while the primary link breaks, the automatic backup function does not occur.
- While using back up interface, Enterprise Edge always calls. Enterprise Edge does not answer an incoming call from a router.
- Support for callback configuration is not provided.

Configuring Unified Manager Settings 4

Configuring Unified Manager includes:

- Configuring system settings
- Configuring resources
  - LAN settings
  - WAN settings
  - MSC settings
  - Telephony (PBX) settings
- Configuring services
  - DHCP settings
  - DNS settings
  - Web caching/proxy
  - Routing settings
- SNMP settings
- Quality of Service (QoS) settings
- VoIP settings
- Quality Measure of Service (QMoS)
- Configuring Unified Manager settings
  - Options settings
  - User Manager settings
  - Alert Manager settings

Accessing system, resources, services and management settings on Unified Manager

You can access Unified Manager system, resources, services and management settings from:

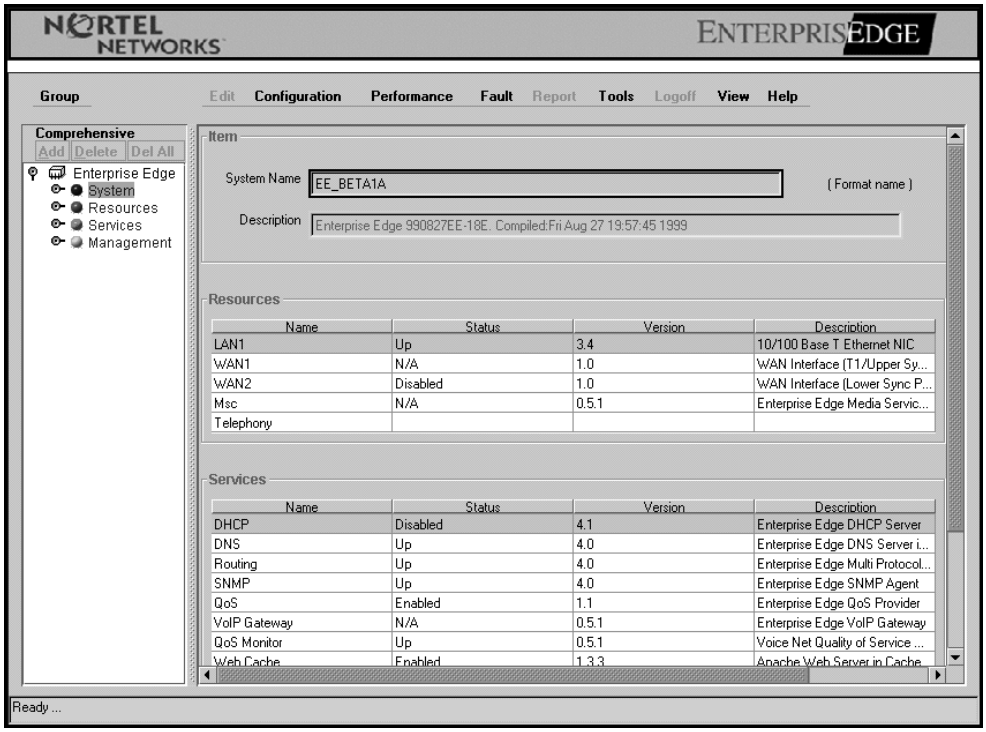
- the menu
  or
- the navigation tree

Configuring system settings

1. Click **Group** and then click **Systems** or **Comprehensive**.

2. On the navigation tree click the **Enterprise Edge** key and then click the **System** key.
   The screen displays the available Enterprise Edge item settings, resources and configurable resource services.

3. Configure item settings using Unified Manager and the resource services from the menu.
   Scroll to see any settings that are not displayed.


NORTEL NETWORKS
ENTERPRISE EDGE
Group
Edit Configuration Performance Fault Report Tools Logoff View Help
Comprehensive
Add Delete Del All
Enterprise Edge
System
Resources
Services
Management
Item
System Name EE_BETA1A
(Format name)
Description Enterprise Edge 990827EE-18E. Compiled:Fri Aug 27 19:57:45 1999
Resources
Name Status Version Description
LAN1 Up 3.4 10/100 Base T Ethernet NIC
WAN1 N/A 1.0 WAN Interface (T1/Upper Sy...
WAN2 Disabled 1.0 WAN Interface (Lower Sync P...
Msc N/A 0.5.1 Enterprise Edge Media Servic...
Telephony
Services
Name Status Version Description
DHCP Disabled 4.1 Enterprise Edge DHCP Server
DNS Up 4.0 Enterprise Edge DNS Server i...
Routing Up 4.0 Enterprise Edge Multi Protocol...
SNMP Up 4.0 Enterprise Edge SNMP Agent
QoS Enabled 1.1 Enterprise Edge QoS Provider
VoIP Gateway N/A 0.5.1 Enterprise Edge VoIP Gateway
QoS Monitor Up 0.5.1 Voice Net Quality of Service ...
Web Cache Enabled 1.3.3 Apache Web Server in Cache
Ready ...

The Unified Manager system settings are:

Setting	Definition
System Name	Lets users specify the system name of the Enterprise Edge, Unified Manager.
Description	Shows a description of the Enterprise Edge Unified Manager installed system.
Resources	A configurable listing of all resources installed on the Enterprise Edge Unified Manager system.
Services	A configurable listing of services available for each resource on the Enterprise Edge Unified Manager system.

The resources and resource services are:

Column	Definition
Name	Shows each configurable resource service.
Status	Shows the status of each configurable resource service.
Version	Shows the version of each configurable resource service.
Description	Shows a brief description of each configurable resource service.

System name

Unified Manager often shows an example of how to format information to the right of the box. Type the information in that format.

To enter the system name:

1. In the **System Name** box type the system name.

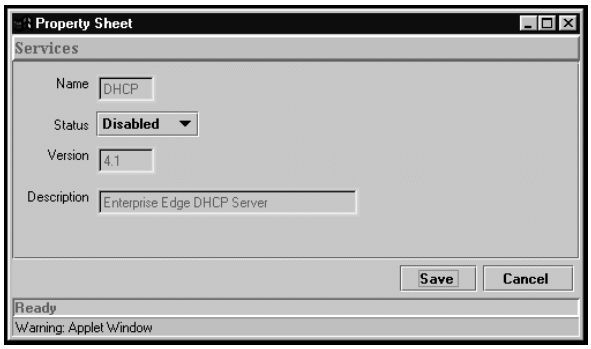
2. Press the **Tab** key to save your changes.

System resource services

1. In the **Resource** options, click the resource you want to configure.

2. In the **Services** options, click the resource service you want to configure. Scroll to see any settings that are not displayed.

3. On the menu click **Configuration** and then click **Modify Services**. The services dialog box appears.



4. From the **Status** list box enable or disable the resource service defined in the Name box.

5. Click the **Save** button to return to Unified Manager.

6. Repeat this process to enable or disable:
   - DHCP
   - DNS
   - Routing
   - SNMP
   - QoS
   - VoIP Gateway
   - Qos Monitor
   - Web Cache
   - Voice Record
   - TAPI Service Provider
   - Voice Service
   - Alarm Service
   - Voice Mail resource service
   - Msc
   - Telephony resource

If a resource service is not highlighted prior to prompting resource modification, an error message appears that asks you to select a row in the table. Click the **OK** button to continue.

Status fields, where available, are the accumulation of 'administrative' and 'operational' status’ of the component queried.

The three administrative statuses that can be assumed by a component are:

- Enabled: the component is enabled to operate in its normal mode, with all normal parameters set. When the component is enabled, the component can assume any of its operational statuses.
- Disabled: the component is disabled from operation. None of the component’s operational statuses are valid in this state.
- Paused: the component is enabled and is running but is currently not accepting additional service requests.

The two operational statuses that can be assumed by a component are:

- Up: the component is up and running normally
- Down: the component is down, due to some reason - normal or abnormal, internal or external.

The Status column supports the combined list of these statuses:

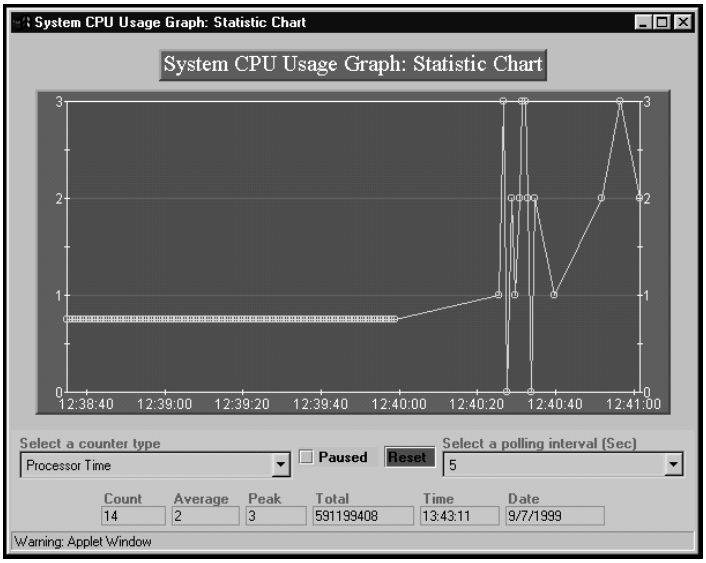
- Up: This value is read-only. It indicates that the component is enabled and is operating normally. For a component like a network interface, this means the interface is enabled and connected to a valid link. For a service like DHCP, it means that the service is enabled and is running normally.
- When the current status is 'Up', setting it to 'Enabled' or 'Continue' where available, is a no-operation. Setting it to 'Disabled' disables the service, by shutting it down and then disabling it. Where available, setting it to 'Paused' pauses the service.
- Down: This value is read-only. This value indicates that the user has enabled the component, and the component is unable to operate in an 'Up' state because of normal or abnormal, internal or external errors. For example, if a network interface is not in an 'Up' state because of no connection to an actual physical link, it is a normal, external error. If a service like DHCP service is not in an 'Up' state because of internal errors, it is an abnormal, internal error.
- When the current status is 'Down' setting it to 'Enabled' attempts to bring it to 'Up' state again. As a result it may stay at a 'Down' state. Setting it to 'Disabled' disables the service. Where available, setting it to a 'Paused' or continued state fail as the service is not yet running.
- Enabled: This value is write-only. This value never appears when read. For a service that is enabled, one of its operational statuses (that is, Up or Down) appears when its Status field is read.

- When this value is set, it indicates that the user wants to enable the corresponding component and bring it to an 'Up' state. It is probable that the first happens. The second action depends on the component. For a network interface, the 'Up' state does not happen unless user connects a link to the interface. For a service this may not happen only if the system encounters an error of some kind during the requested action.
- Disabled: This value can be either read or set. When read, this indicates that the component is disabled from operation. When set, it indicates the same, in addition to taking the component to a 'Down' state before disabling.
- Paused: This value can be either read or set. When read, this indicates that the service is enabled and is given the command to pause. When set, it indicates the same, pausing the service further.
- Continue: This value can only be set. It can be set only when the service in a Paused state. It resumes paused service.

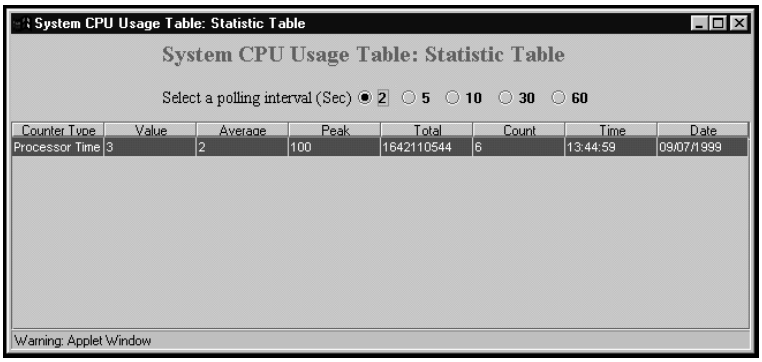
System performance graphs and tables

To access the system performance graphs and tables:

1. On the menu click **Performance** and then click **System CPU Usage Graph**. The System CPU Usage Graph appears.



2. On the menu click **Performance** and then click **System CPU Usage Table**. The System CPU Usage Table appears.


System CPU Usage Table: Statistic Table
System CPU Usage Table: Statistic Table
Select a polling interval (Sec) 2 5 10 30 60
Counter Type Value Average Peak Total Count Time Date
Processor Time 3 2 100 1642110544 6 13:44:59 09/07/1999
Warning: Applet Window

3. Access the Memory Usage graph and Memory Usage table by following the steps for System CPU Usable Graphs and Tables.

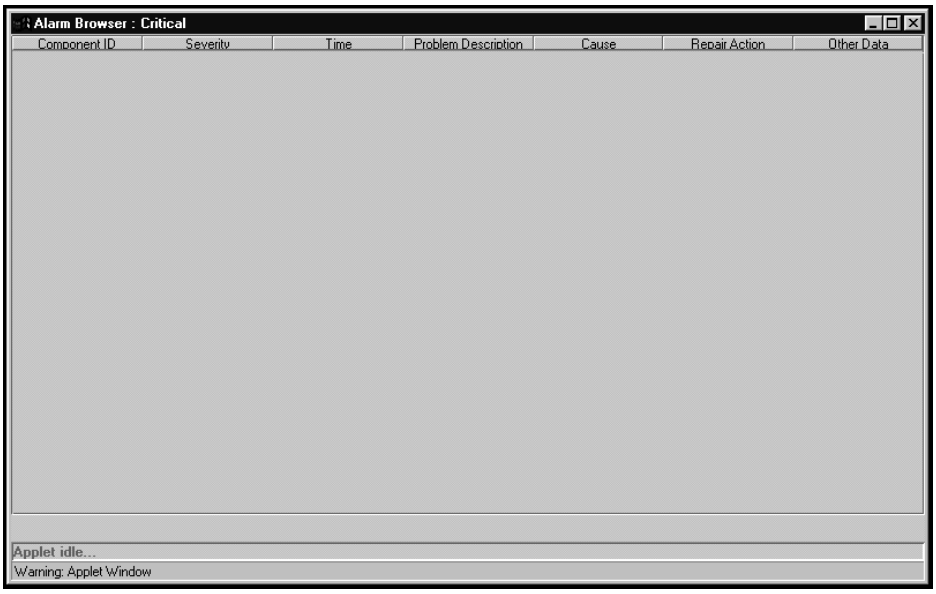
For information on using performance tables and graphs, refer to Graphs and tables on page 154.

System Fault Alarm Banner

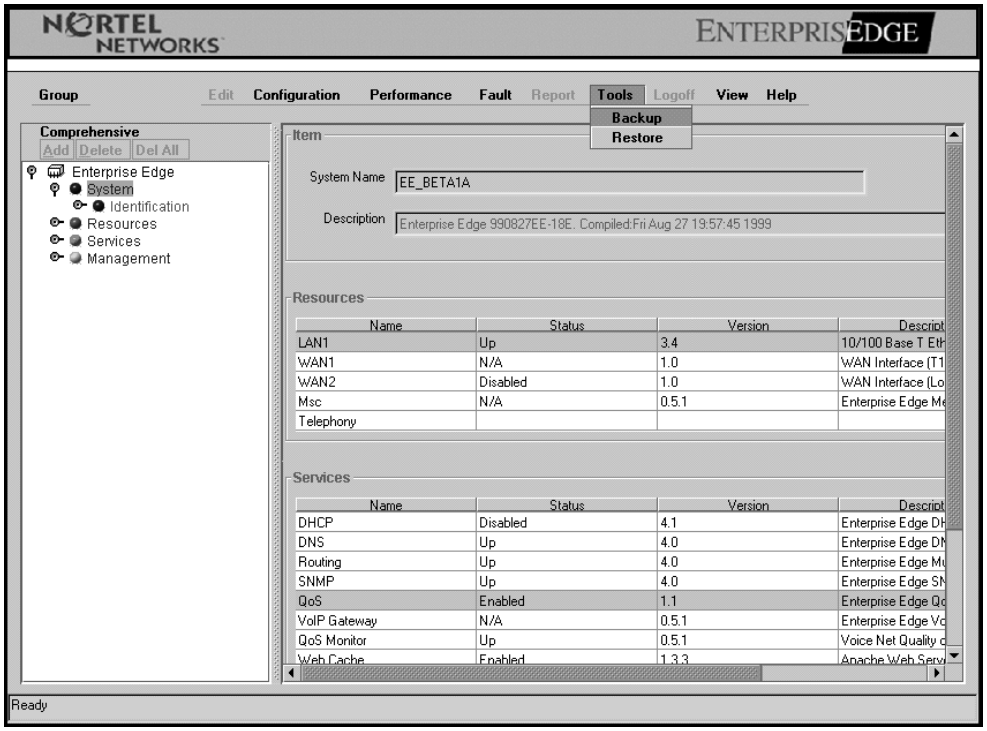
To access the system fault alarm banner:

1. On the menu click **Configuration** and then click **Fault**.
   The Alarm Banner dialog box appears.

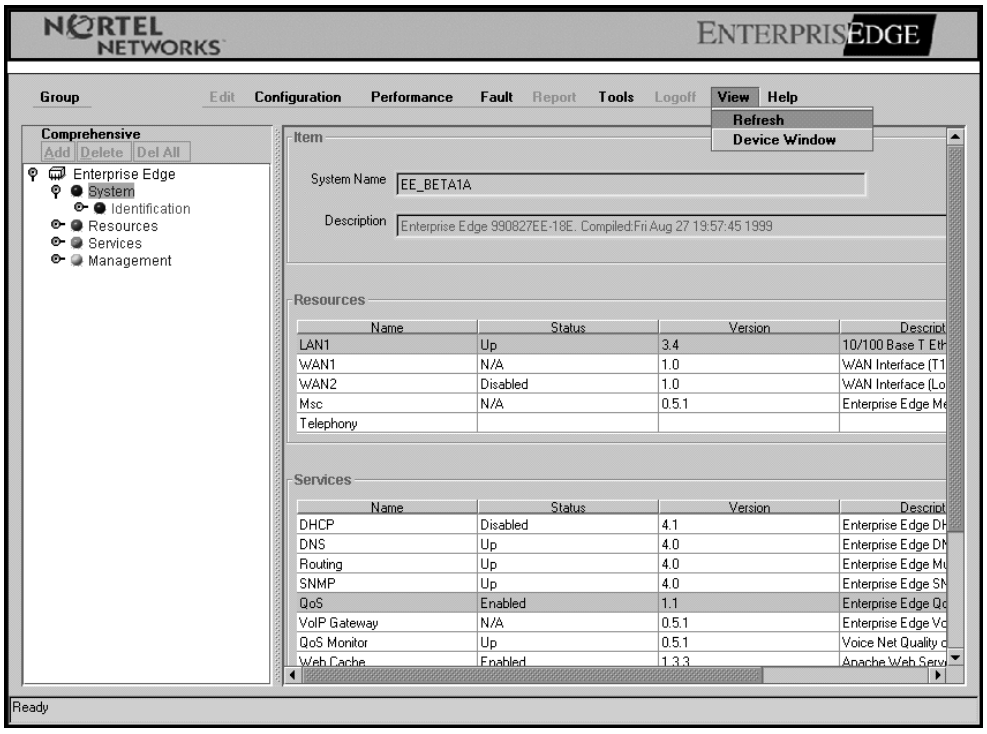
System Alarm Banner Message Listing



Accessing System Tools



Accessing System Save Options



System name, date and time

To change the system name, date and time:

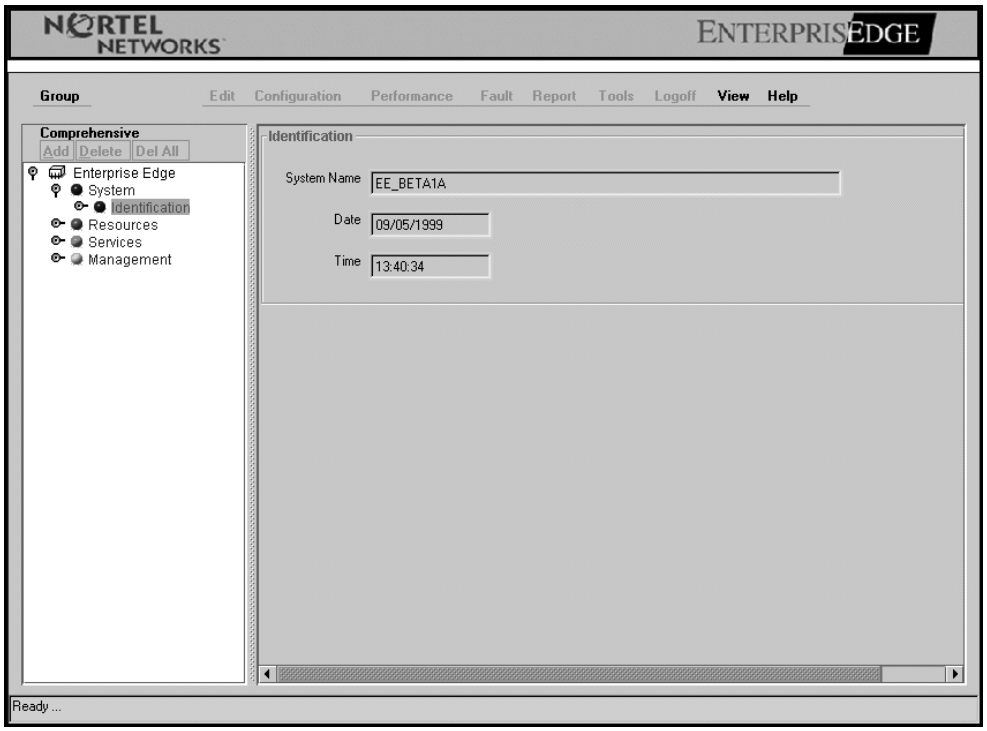
1. Click the **System** navigation key to expand the navigation tree.
   The System Settings dialog box appears.
   Clicking the System navigation key expands the navigation tree but doesn't display the summary of configurable Identification resources.

   The System Settings are:

Setting	Definition
Name	Lets users specify the name for the Enterprise Edge system. The Enterprise Edge system must have a unique name in the connected network (LAN or WAN) so that no two Enterprise Edge servers that can reach each other through IP network do not have the same name. The name must be less than 15 characters in length, cannot contain special characters like "/;," etc.
Date	Lets users set the current date for the Enterprise Edge system. Because the value for the date changes, save the changes as soon as the new date is entered.
Time	Lets users set the current time for the Enterprise Edge system. Because the value for the time keeps changing, save the changes as soon as the new time is entered. Use the 24-hour format to set the date. The seconds field is optional.

2. On the navigation tree click **Identification** to view the available system settings to configure.
   The System Identification dialog box appears.

Note: Clicking the Identification navigation key causes the key to disappear. You must click Identification to display the configurable system settings.



3. In the **System Name** box type the system name.
4. In the **Date** box type the current date.
5. In the **Time** box type the current time.
6. Press the **Tab** key to save the changes.
7. Clicking the **System** navigation key to close the navigation tree.

Configuring Resources Settings

5

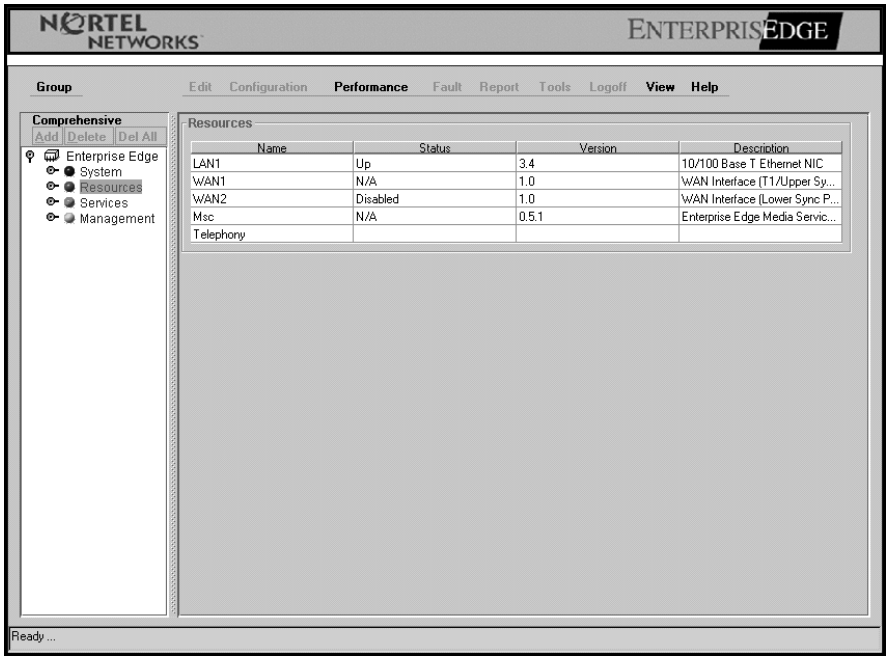
Configuring Resources includes configuring:

- LAN
- WAN Settings
- MSC Settings
- Telephony (PBX) Settings

To open the Unified Manager Resources screen:

1. On the menu click **Group** and then click **Resources** or **Comprehensive**.

2. On the navigation tree click **Enterprise Edge** and then click the **Resources** keys.
   The available Enterprise Edge resources appear.



3. Click the **Resources** navigation key to expand the navigation tree.

The columns that are displayed when the system, resources, services, or management settings are activated are:

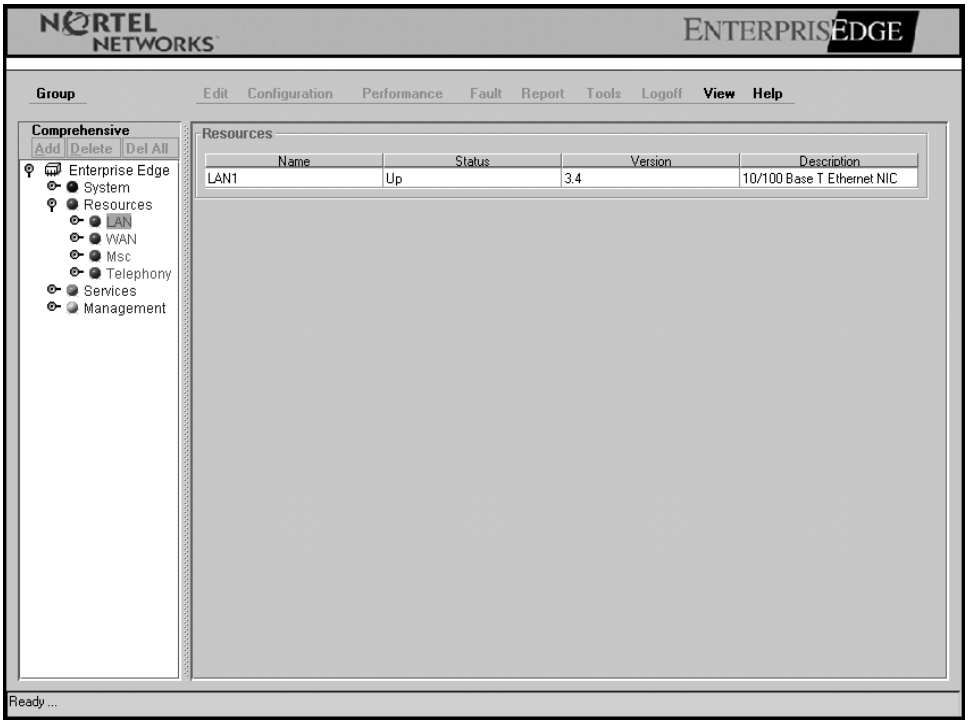
Column	Definition
Name	The name column lists the available configurable resources.
Status	The status column lists the operating status of each configurable resource.
Version	The version column lists the version of each configurable resource.
Description	The description column gives a brief description of the interface for each configurable resource.

LAN

You configure LAN resource settings from Unified Manager.

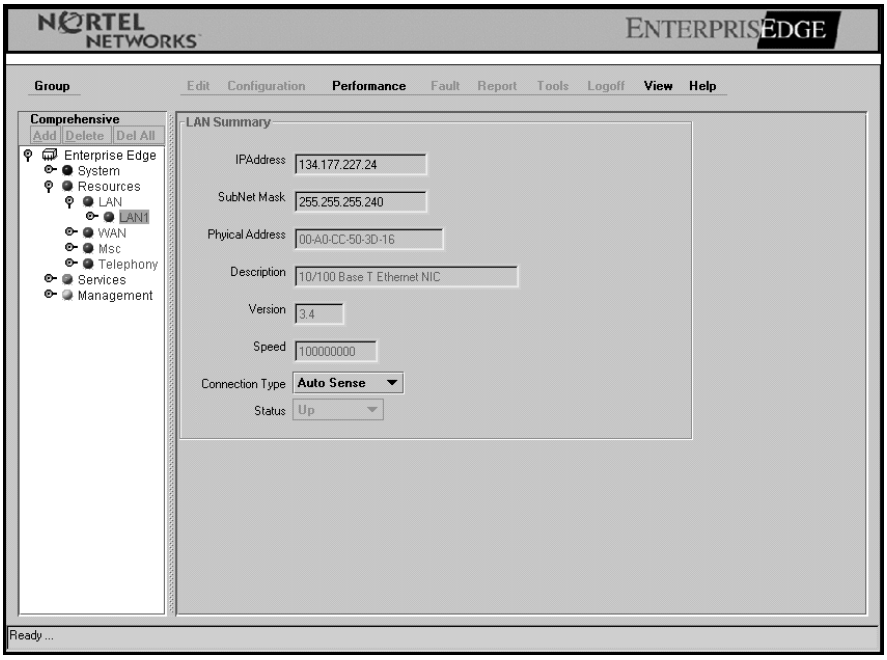
If your Enterprise Edge server has more than one LAN interface, multiple items appear under LAN resources. To configure other LAN interfaces, follow the instructions given here for LAN1.Choose **LAN** from the navigation tree to view the available LAN resources to configure.

Note: Clicking the LAN navigation key expands the navigation tree, but doesn't display the summary of configurable LAN resources.



4. Click the **LAN** navigation key to expand the navigation tree.

5. On the navigation tree click **LAN1**.
   Clicking the LAN1 navigation key causes the key to disappear. You must click LAN1.
   The LAN Summary screen appears.



The LAN Summary settings are:.

Setting	Definition
IP Address	Lets users specify the IP address of the LAN interface in a valid dot format. Type the address in the following format: 10.10.10.1. The value for this field is valid only if the LAN interface is enabled.
SubNet Mask	Lets users specify the subnet mask of the LAN interface. Type the data in the following dot format 255.255.255.0.
Physical Address	Lets users to view the physical address of the LAN interface. If the IP Address or subnet mask of the LAN interfaces changes, a DHCP scope associated with the LAN interface is created in the DHCP server running on the Enterprise Edge server. This scope contains all necessary parameters to the clients of the DHCP server configured so that they use Enterprise Edge as their default gateway and a WINS server. The scope also contains default parameters for the range of the addresses, based on the address of the Enterprise Edge interface and subnet mask. Navigate through the services screen in the user interface to see DHCP settings for the scope.
Description	Lets users view a description of the network interface card supporting the LAN interface.
Version	Lets users view the version indicator of the LAN interface.
Speed	Lets users view the speed of the connection to the LAN interface. The value for this field is valid only if the LAN interface is enabled.

Setting	Definition
Connection Type	Lets users specify the connection type to the LAN interface. The following values are supported and are interpreted as follows: Auto Sense: The interface uses 'auto negotiation' protocol to choose the maximum possible speed of the connection. Depending upon the connected device, the interface can choose '100 MB' or '10MB', full-duplex, or half-duplex. The receiving end's speed and connection type determines the mode of transmission. For example, if the receiving end is another PC port, or a bridge/switch port, the full duplex of operation is possible; if the receiving end is a shared media port (like hub port), only half-duplex of mode is possible. 10 MB Half: Speed is set to 10 MB/s and mode to half-duplex. 10 MB Full: Speed is set to 10 MB/s and mode to full-duplex 10 MB Auto: The speed is set to 10 MB/s and the mode is automatically chosen by the interface, using auto-negotiation protocol. This mode is chosen to limit the maximum traffic coming in to Enterprise Edge to 10 MB, while enabling the auto-negotiation feature for easier interconnection. Usually, you limit the incoming traffic if you notice that the bursty traffic from the connected LAN is degrading the quality of voice calls carried through VoIP over WAN. Though the LAN traffic gets lower priority in Enterprise Edge, their high rate of arrival to the Enterprise Edge server generates too may interrupts in the system that cause degraded quality in voice calls carried as VoIP. 100 MB Half: Speed is set to 100 MB/s and mode to half-duplex 100 MB Full: Speed is set to 100 MB/s and mode to full-duplex.
Status	Lets users view the current status of the LAN interface. The possible states are: Up: the resource is operational. Down: the resource is not operational.

Consult your System Administrator for the appropriate configuration information before changing the settings

To modify the configuration of the LAN1 settings:

1. In the **IP Address** box type the IP address.
   An example of how to format the information is shown at the right of the box.

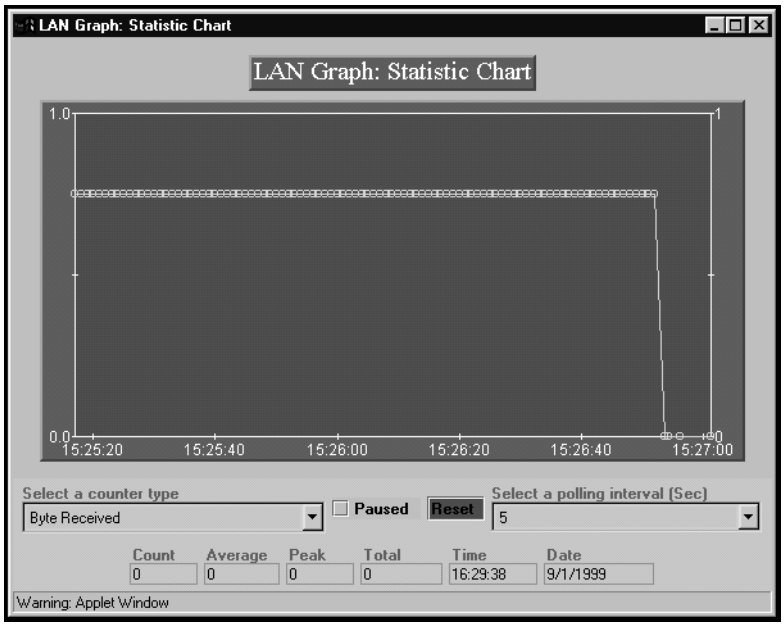
2. In the **SubNet Mask** box type the subnet mask

3. From the **Connection Type** list select the connection type.

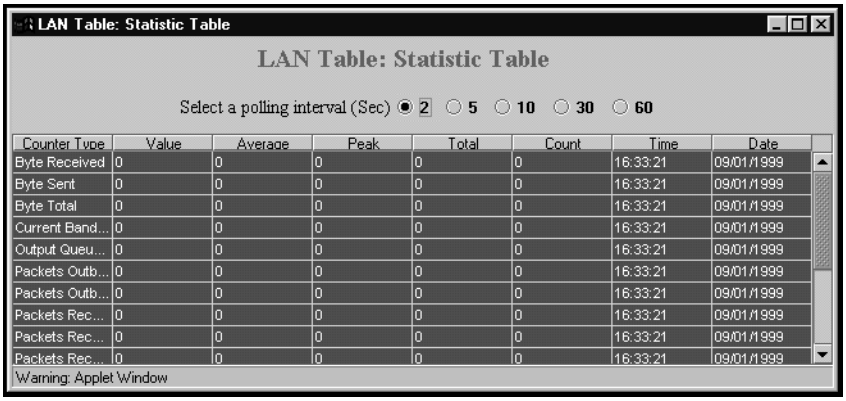
4. Press the **Tab** key to save the settings.

To view LAN performance:

1. On the menu, click **Performance** and then click **LAN Graph**. The LAN Graph Statistic Chart appears.



2. On the menu, click **Performance** and then click **LAN Table**. The LAN Graph Statistic Table appears.


LAN Table: Statistic Table
LAN Table: Statistic Table
Select a polling interval (Sec) 2 5 10 30 60
Counter Type
Value
Average
Peak
Total
Count
Time
Date
Byte Received 0 0 0 0 0 16:33:21 09/01/1999
Byte Sent 0 0 0 0 0 16:33:21 09/01/1999
Byte Total 0 0 0 0 0 16:33:21 09/01/1999
Current Band... 0 0 0 0 0 16:33:21 09/01/1999
Output Queu... 0 0 0 0 0 16:33:21 09/01/1999
Packets Outb... 0 0 0 0 0 16:33:21 09/01/1999
Packets Outb... 0 0 0 0 0 16:33:21 09/01/1999
Packets Rec... 0 0 0 0 0 16:33:21 09/01/1999
Packets Rec... 0 0 0 0 0 16:33:21 09/01/1999
Packets Rec... 0 0 0 0 0 16:33:21 09/01/1999
Warning: Applet Window

For information on using performance tables and graphs, refer to Graphs and tables on page 154.

3. Click the **LAN** navigation key to close the navigation tree.

WAN primary links

You configure WAN resource settings from Unified Manager.

WAN Interfaces have names like WAN1 and WAN2. If your Enterprise Edge server has a permanent WAN card, WAN1 and WAN2 are interfaces from this card. They can run Frame Relay or PPP on a permanent WAN Link operating at T1 speed. Click on these interfaces to see their description.

If your Enterprise Edge server also contains a modem card with dial up interfaces, they appear as WAN3, WAN4 and so on. Click on these interfaces to see their description. If your Enterprise Edge server does not have a WAN card, dial-up interfaces appear as WAN1, WAN2 and so on.

The configurable parameters and options are different for permanent WAN links and for dial-up WAN links. In this document, it is assumed that WAN1 and WAN2 are permanent WAN links and WAN3 and others, are be dial-up interfaces.

To view the WAN primary links

1. Click **WAN** to view the available WAN resources to configure.

2. Click the **WAN** navigation key to expand the navigation tree.
   Clicking the WAN navigation key expands the navigation tree but doesn't display the summary of configurable WAN resources.

3. On the navigation tree, click **WAN1** or **WAN2.**
   Clicking the WAN1 or WAN2 navigation key causes the key to disappear. You must click WAN1 or WAN2.
   The screen displays the WAN Summary, WAN Line Parameters, WAN Frame Relay Parameters, WAN PPP Parameters, and PVC Congestion Control settings.

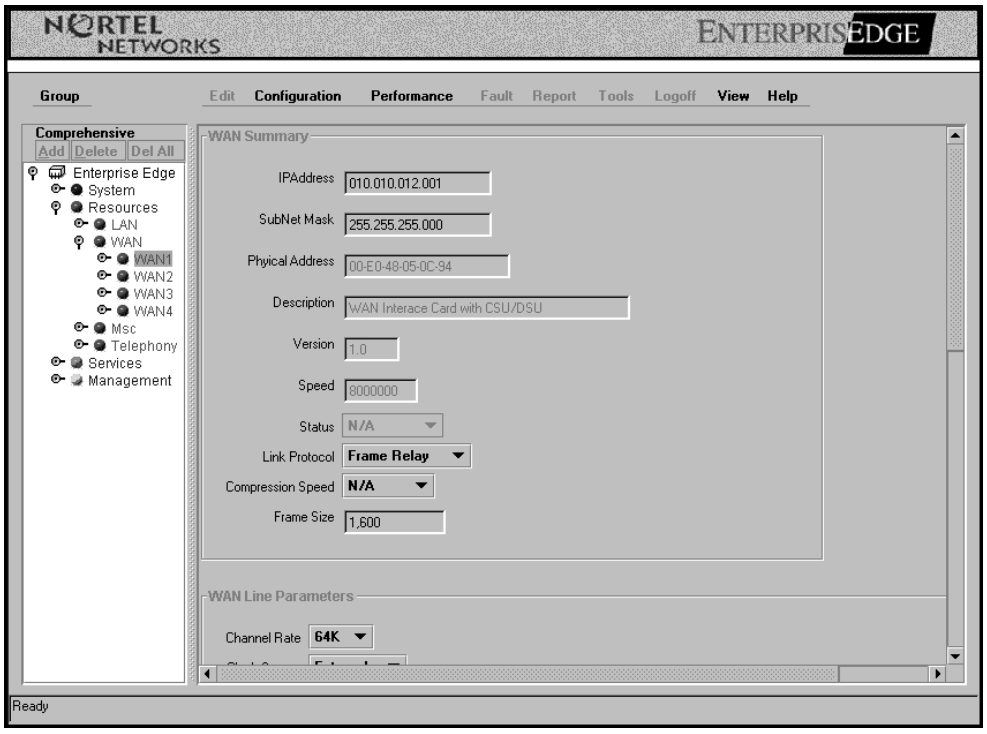
   Note: The WAN Frame Relay Parameters do not appear unless frame relay is chosen as your link protocol in the WAN Summary. To display the WAN frame relay parameters, from the **Link Protocol** list box select **Frame Relay**. Press the **Tab** key to update the screen. A configurable WAN Frame Relay Parameters dialog does not appear unless the current link protocol is PPP.

4. Scroll to view any settings that are not displayed.

5. Configure the WAN Summary, WAN Line Parameters, WAN Frame Relay Parameters and WAN PPP Parameters screen from Unified Manager. Configure the PVC congestion control screen using the menu.

If your current link protocol is Frame Relay, you may have to configure WAN Frame Relay parameters and PVC Congestion Control entries. If your current link protocol is PPP, you may have to configure WAN PPP Parameters.

If the WAN port you are configuring is a T1 Port, you may have to configure WAN Line Parameters. If the port you are configuring is a synchronous (Sync) port, WAN Link Parameters have no effect, and are ignored. See the description of the port in WAN Summary section to see which port you are configuring.



WAN Primary Link Summary Parameters

The WAN summary settings are:

Setting	Definition
IP Address	Lets users specify the IP address of the WAN interface in a valid dot format. Type the data in the following dot format: 10.10.10.1.
SubNet Mask	Lets users specify the subnet mask in a valid dot format of the WAN interface. Type the data in the following dot format 255.255.255.0.
Physical Address	Shows the physical address of the WAN interface.
Description	Shows the description of the network interface card that supports the WAN interface.
Version	Shows the version indicator of the WAN interface.
Speed	Shows the operational speed of the WAN interface.
Status	Shows the current resource status of the WAN interface. The possible states are: Up: the resource is operational. Down: the resource is not operational.
Link Protocol	Lets users specify PPP or frame relay protocol. If you change the link protocol, the configuration screen changes to include fields corresponding to the link protocol you choose. To ensure proper operation, always refresh the page by clicking **View** and then **Refresh**.
Compression Speed	Lets users specify fast, medium, normal, slow, or no data compression configuration.
Frame Size	Lets users specify the maximum frame size for the layer-2 packet carried on this port.

To modify the configuration of the WAN1 or WAN2 summary screen:

6. In the **IP Address** box type the IP address.
7. In the **SubNet Mask** box type the subnet mask.
8. From the **Link Protocol** list box choose **Frame Relay** or **PPP**.

   Note: If you choose Frame Relay, press the **Tab** key to update the screen. A configurable WAN Frame Relay Parameters screen appears.

9. From the **Compression Speed** list box select the compression speed.
10. In the **Frame Size** box type the frame size.
11. Press the **TAB** key to save your settings.

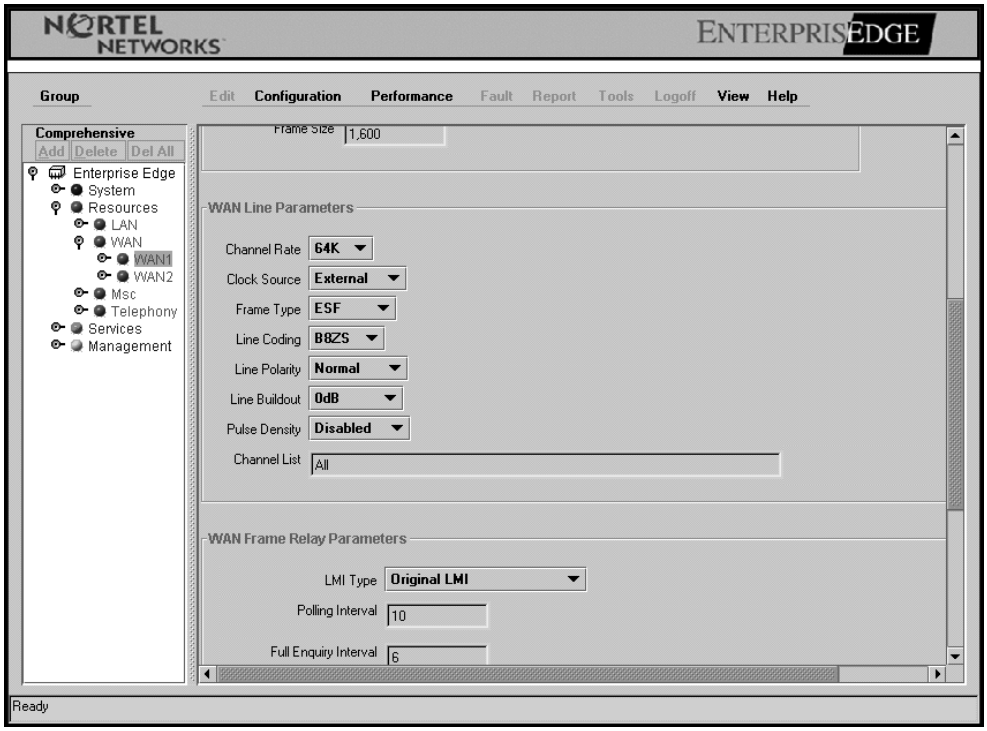
WAN Primary Link Line Parameters

The WAN Link Line Parameters settings are:

Setting	Definition
Channel Rate	Lets users set the data rate for each of the DS0 channels in the T1 line.
Clock Source	Lets users set an internal or external T1 clock source.
Frame Type	Lets users set the type of framing to be adopted in the T1 line. You can select either SF(D4) or ESF for frame type. SF(D4) transmits superframes consisting of 12 individual frames. ESF transmits superframes consisting of 24 individual D4 frames and provides enhanced signaling and synchronization. ESF lets you testing the digital line while it is in use. Always use the frame type that the equipment at the receiving end expects.
Line Coding	Lets users set the type of encoding used in the T1 line. You can select either B8ZS or AMI for this parameter. B8ZS (Bipolar with 8 Zero Substitution) line coding replaces a block of eight consecutive binary zeros with an 8-bit B8ZS code containing bipolar violations in the fourth and seventh bit positions of the substituted code. In the receiving direction, the B8ZS code is detected and replaced with eight consecutive binary zeros. AMI line coding is also bipolar: a binary zero is transmitted as zero volts, and a binary 1 is transmitted as either a positive or negative pulse, opposite in polarity to the previous pulse. Always use the line coding method that the equipment at the receiving end expects.
Line Polarity	Lets users set normal or inverted line polarity in the T1 line. The option inverted is meaningful only if LineCoding is AMI.
Pulse Density	Lets users control whether the DSU/CSU maintains the minimum level of 1s on the line for AMI encoding.
Channel List	Lets users create a list of channels used in the T1 line. You can specify multiple channel numbers in a comma-separated list. Each item in the list can contain a range of channel numbers, with the limits of the range separated by a hyphen character. For example, this is a valid value for channel list: 3,5,6,10-15,18,20-23. If you use all of the channels, specify it by using the string All.

To modify the configuration of the WAN1 or WAN2 Line Parameters screen:

1. Scroll to view the WAN Line Parameters screen.



2. From the **Channel Rate** list box select the channel rate.

3. From the **Clock Source** list box select the clock source.

4. From the **Frame Type** list box select the frame type.

5. From the **Line Coding** list box select the line coding.

6. From the **Line Polarity** list box select the line polarity.

7. From the **Pulse Density** list box select the appropriate pulse density and close the list box.

8. In the **Channel List** box.type the channel list.
   Specify a list of channels numbers or their ranges separated by a comma or hyphen. Ranges can be mixed with individual entries.

9. Press the **Tab** key to save the settings.

WAN Primary Link Frame Relay Parameters

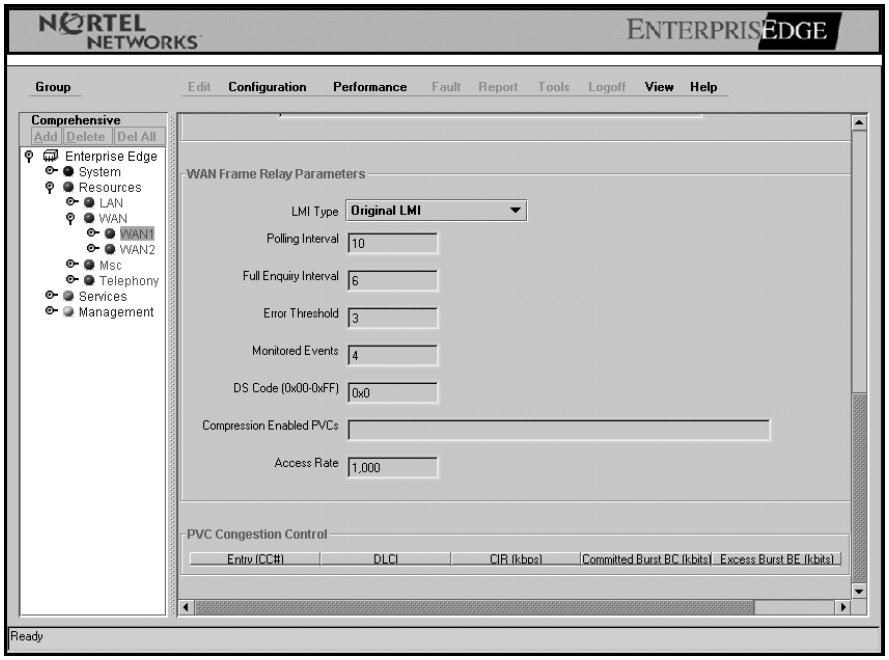
The WAN Frame Relay Parameters are:.

Setting	Definition
LMI Type	Lets users set the type of link management protocol used on this link. This value must match the corresponding value set in the Frame Relay service provider's switch. Permitted values are ANSI, LMI, and CCITT. The default setting is ANSI.
Polling Interval	Lets users set a value, in seconds, as an interval between LMI status inquiry messages. This value must match the corresponding value set in the Frame Relay provider's switch. Permitted values are between 5-30 (in seconds). The default setting is 10.
Full Enquiry Interval	Lets users set the maximum number of LMI Status Enquiry messages sent before sending a Full Status Enquiry request. This value must match the corresponding value set in the Frame Relay provider's switch. Permitted values are between 1 and 255 (in seconds). The default setting is 6.
Error Threshold	Lets users set the maximum number of consecutive failures permitted in LMI Status Enquiry before marking the link non-operational. It is also the number of successful consecutive LMI Status Enquiry messages that must be received before marking a link as operational. Permitted values are between 0 and MAXINT. The default setting is 3.
Monitored Events	Lets users set the number of events sampled for making decisions about the error threshold. Set the number higher than the values set in the error threshold. Permitted values are a number between 0 and MAXINT. The default setting is 4.
DS Code	Lets users set the differentiated services code (DSCode) recognized by the frame relay driver for prioritization. This value is used as a mask value. When an IP packet is sent down, the frame-relay driver checks if the packet's DSCode field (known as TOS byte in earlier documents) has any of the bits specified in this field set (a bitwise AND operation is performed between this field's value and the DSCode field of the IP packet and the result is checked for 0). If any of the bits is set (result is non-zero), the frame relay network is signaled to handle this packet with priority by clearing the 'D/E' (discard eligibility) bit in the frame relay packet header. If none of the bits specified in this field are set in the IP packet header, 'D/E' bit is set in the frame-relay packet header, marking the packet as a likely candidate for packet drop in case of congestion in the frame relay network. This field's value carries the same semantics as the 'differentiated services codepoint' discussed in RFC2474. The least significant two bits are ignored.
Compression Enabled PVCs	Lists PVCs on which compression is enabled. If the compression field is Disabled, the field does not have any meaning. If the compression level Enabled, compression and decompression are performed on the data going to and coming from the PVCs in this list. The value can be a comma-separated list of DLCI numbers. You can specify a range of DLCIs by specifying the lower and upper boundaries by a hyphen. You can mix individual numbers and ranges.

Setting	Definition
Access Rate	Lets users set, in kbps, the maximum access rate on the interface running frame-relay. The frame-relay congestion control engine uses this value to limit or shape traffic. Specify a value computed using the T1 channels available for data communication on the port attached to this interface and their data rates.

To modify the configuration of the WAN Frame Relay Parameters:

1. Scroll to locate the WAN Frame Relay Parameters screen.



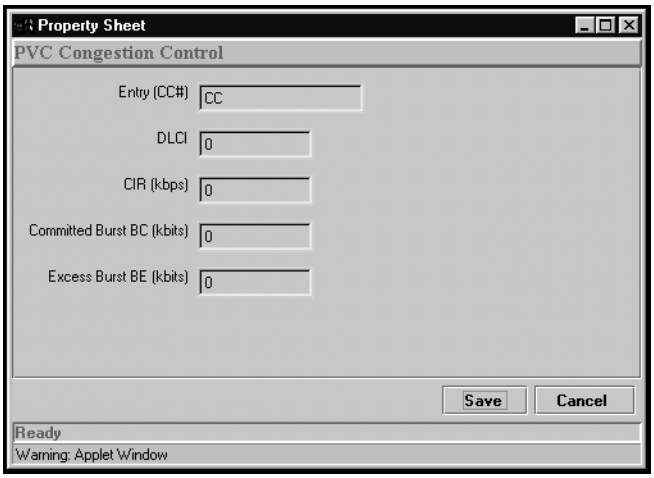
2. From the **LMI Type** list box select the LMI type.
3. In the **Polling Interval** box type the polling interval in seconds.
4. In the **Full Enquiry Interval** box type the full enquiry interval.
5. In the **Error Threshold** box type the error threshold.
6. In the **Monitored Events** box type the appropriate monitored events.
7. In the **DS Code** box type the DS code.
8. In the **Compression Enabled PVCs** box type the compression.
9. In the **Access Rate** box type the access rate in kbps.
10. Press the **Tab** key to save the settings.

The WAN PVC Congestion Control settings are:

Setting	Definition
Entry (CC#)	Uniquely identifies the congestion control entry on the interface. Use the format specified for the entry identifier. It must include the prefix 'CC' followed by a unique number in the table. For example, 'CC2' is a valid number. If you don't use consecutive numbers while adding the entry, the system adjusts them to be consecutive. If you specify an existing entry while adding an entry, the existing entry is modified with new values. While modifying an entry, the name can't be changed.
DLCI	Lets users set the DLCI number for the PVC to be congestion controlled. If a DLCI is not configured, it is not congestion controlled. Enterprise Edge uses one-second intervals to measure this parameter.
CIR	Lets users set, in kbits, the carrier guarantees the router transmits over a specified time interval when congestion is not present. Enterprise Edge uses one-second intervals to measure this parameter.
Committed Burst (bC)	Lets users to define the number, in kbits, of bits the router transmits over a specified time interval if congestion is present. Usually this value is set for 1/4 the value of the CIR. Enterprise Edge uses one-second intervals to measure this parameter.
Excess Burst (Be)	Combined with the committed burst rate, lets users set, in kbits, the maximum number of bits the router transmits over a specified time interval if there is no congestion. Both Be and bC must be less than or equal to the line speed.

To add PVC congestion control:

1. On the menu click **Configuration** and then click **Add PVC Congestion Control**.
   The PVC Congestion Control dialog box appears.
   If an entry range has not been selected an error message appears.



2. In the **Entry (CC#)** box type the entry that looks like “CCxx” where “xx” is a unique integer.

3. In the **DLCI** box type the DLCI.
4. In the **CIR (kbps)** box type the CIR in kbps.
5. In the **Committed Burst BC (kbits)** box type the committed burst in kbits.
6. In the **Excess Burst BE (kbits)** box type the excess burst in kbits.
7. Click the **Save** button to return to Unified Manager.

To modify PVC congestion control:

1. Click an entry in the PVC Congestion Control range.
2. On the menu click **Configuration** and then click **Modify PVC Congestion Control**.
   The PVC Congestion Control dialog box appears.
3. Click any box that requires modification and type the necessary changes.
4. Click the **Save** button to return to Unified Manager.

To delete PVC congestion control:

1. Click an entry in the PVC Congestion Control range.
2. On the menu click **Configuration** and then click **Delete PVC Congestion Control**.
   A message appears that asks you to confirm the deletion.
3. Click the **Yes** button to delete PVC congestion and return to Unified Manager.

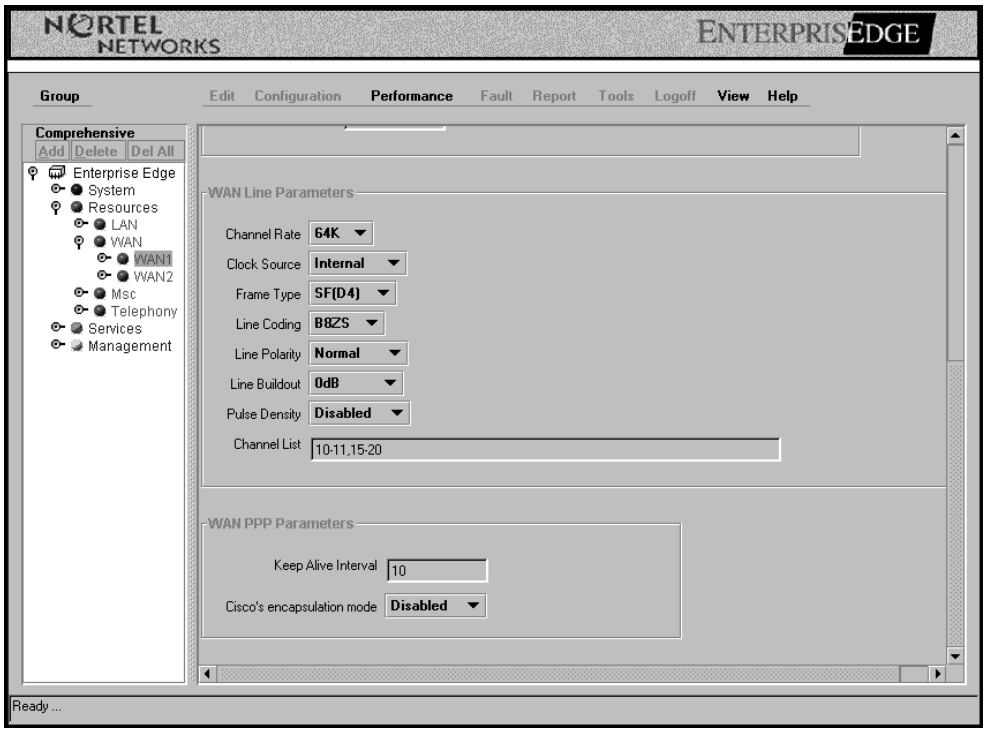
WAN Primary Link PPP parameters

The WAN PPP Parameters are:

Setting	Definition
Keep Alive Interval	Lets users specify the interval between kept alive messages sent when there is no regular traffic on the PPP link.
Cisco's Encapsulation Mode	Lets users enable or disable the Cisco compatibility mode.

To set the WAN PPP parameters:

1. Scroll to the WAN PPP Parameters screen.
   The WAN PPP Parameters screen appears.



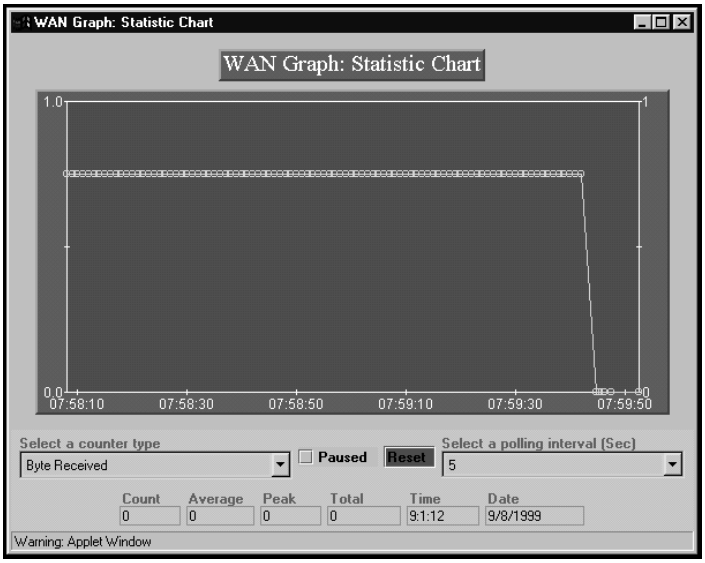
2. In the **Keep Alive Interval** box type the keep alive interval in seconds.

3. From the **Cisco's Encapsulation Mode** list box to enable or disable the Cisco compatibility mode.

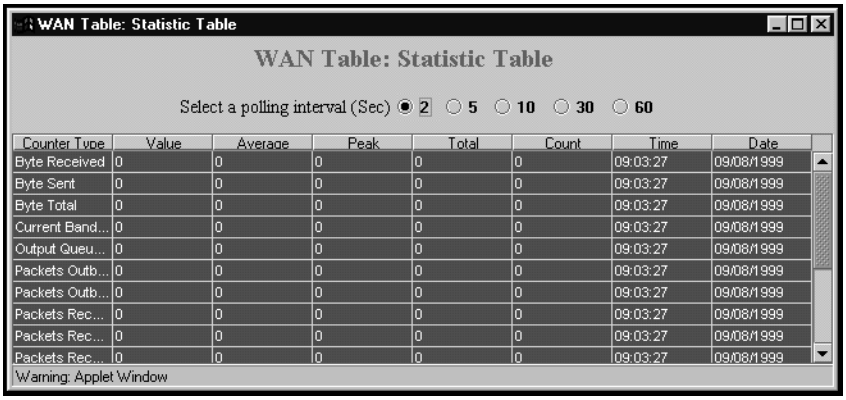
WAN Primary Link performance graphs and tables

To access the WAN Primary Link performance graphs and tables:

1. On the menu click **Performance** and then click **WAN Graph**.
   The WAN Graph Statistic Chart appears.



2. On the menu click **Performance** and then click **WAN Table**.
   The WAN Table: Statistic Table appears.


WAN Table: Statistic Table
WAN Table: Statistic Table
Select a polling interval (Sec) 2 5 10 30 60
Counter Type
Value
Average
Peak
Total
Count
Time
Date
Byte Received 0 0 0 0 0 09:03:27 09/08/1999
Byte Sent 0 0 0 0 0 09:03:27 09/08/1999
Byte Total 0 0 0 0 0 09:03:27 09/08/1999
Current Band... 0 0 0 0 0 09:03:27 09/08/1999
Output Queu... 0 0 0 0 0 09:03:27 09/08/1999
Packets Outb... 0 0 0 0 0 09:03:27 09/08/1999
Packets Outb... 0 0 0 0 0 09:03:27 09/08/1999
Packets Rec... 0 0 0 0 0 09:03:27 09/08/1999
Packets Rec... 0 0 0 0 0 09:03:27 09/08/1999
Packets Rec... 0 0 0 0 0 09:03:27 09/08/1999
Warning: Applet Window

For information on using the WAN statistic chart and the WAN statistic table, refer to Graphs and tables on page 154.

WAN Backup Links

WAN3 and WAN4 are dial up interfaces that are configured according to the V.90 modem in the Enterprise Edge server. You must click WAN3 to see its description.

Dial up WAN Links always use PPP as link-layer protocol. They must be connected to PPP capable RAS Servers that can run RIP or can accept static routes for proper operation.

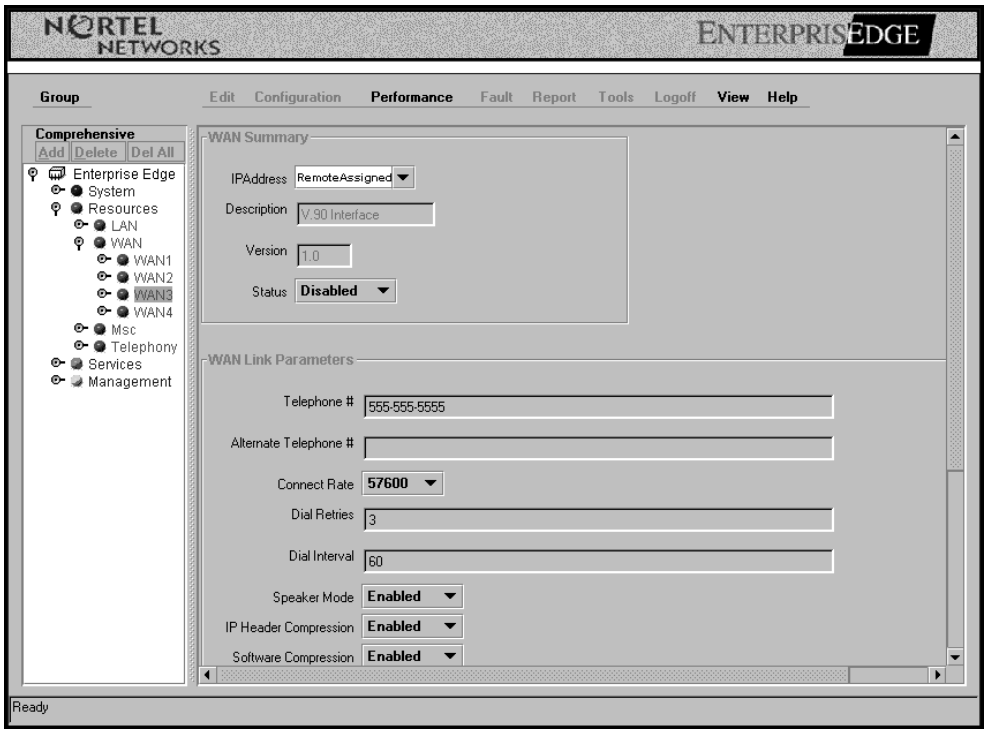
1. On the navigation tree, click **WAN3**.
   Clicking the WAN3 navigation key causes the key to disappear. You must choose WAN3.
   The WAN Summary, WAN Link Parameters, and WAN Access Parameters screen appears.

2. Scroll to see any settings that are not displayed.

1. From the **IP Address** list box select the appropriate IP address assignment or type a new value.

2. From the **Status** list box enable or disable the connection to the backup link.

3. Press the **Tab** key to save the settings.



WAN Backup Link Summary Parameters

The WAN Summary contains these settings:

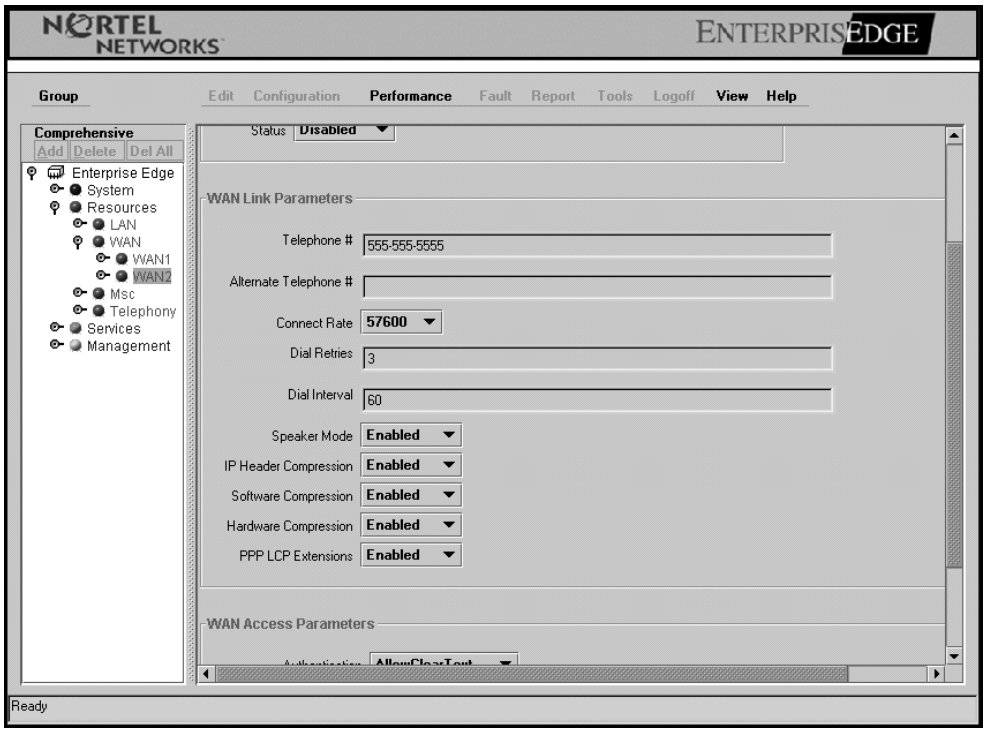
Setting	Definition
IP Address	Lets users set the IP address of the modem interface in a valid dot format when it connects. Users can set a fixed IP Address for the dial-up interface. If a fixed address is specified, it is used by Enterprise Edge to connect to the receiving end. Instead, users can choose RemoteAssigned to indicate that Enterprise Edge must obtain an IP address from the remote end and use it. The address obtained depends on the RAS server that the Enterprise Edge server connects to.
Description	Shows a description for the subsystem that is encapsulated by the DLL.
Version	Shows the version for the subsystem that is encapsulated by the DLL.
Status	Lets users set the modem interface resource status. The possible states are: Up: the auto WAN backup service is enabled and the dial-up link is currently connected. Down: the auto WAN backup service is enabled and the dial-up link is currently disconnected. Enabled: the interface is enabled for use by the auto-backup server. Disabled: the auto WAN backup service is disabled.

WAN Backup Link Parameters

The WAN Link Parameters are:

Setting	Definition
Telephone Number	Lets users specify a telephone number to be used to connect using the modem interface. If needed, include area codes, if any, and all necessary digits to dial an external number.
Alternate Telephone Number	Lets users specify an alternate number to be used to connect using the modem interface. Include area codes, if any, and all necessary digits to dial an external number.
Connect Rate	Lets users specify the initial speed (in bits per second) for the modem to connect. Set to the maximum permissible value for best results. Permitted values: 57600, 38400, 19200, 9600, 4800. Note: This is the initial rate, actual rate is always negotiated.
Dial Retries	Lets users specify the number of tries the system attempts to make a link operational before marking it non-operational. A positive number must be used.
Dial Interval	Lets users specify the interval, in seconds, between successive attempts to make a link operational.
Speaker Mode	Lets users enable or disable the speaker during initial link establishment.
IP Header Compression	Lets users enable or disable IP header compression. To function, the receiving end must utilize this feature to work.
Software Compression	Lets users enable or disable data compression in the software, instead of the modem. For dial-up connections, Unified Manager uses Microstate Point-to-Point Compression algorithm (MPPC).
Hardware Compression	Lets users enable or disable data compression in the hardware instead of the software.
PPP LCP Extensions	Lets users specify whether or not to enable or disable PPP LCP extensions that include Time-Remaining, Identification, and Callback features. The Callback feature is not supported even if LCP extension is enabled.

1. Scroll to see the WAN Link Parameters settings.



2. In the **Telephone #** box type your telephone number choice.

3. In the **Alternate Telephone #** box type your alternate telephone number choice.

4. From the **Connect Rate** list box select your connection rate choice.

5. In the **Dial Retries** box type the number of times to attempt dialing if the connection fails.

6. From the **Speaker Mode** list box select your speaker mode choice.

7. From the **IP Header Compression** list box select enable or disable.

8. From the **Software Compression** list box select enable or disable.

9. From the **Hardware Compression** list box select enable or disable.

10. From the **PPP LCP Extensions** list box select enable or disable.

11. Press the **Tab** key save the settings.

WAN Backup Access Parameters

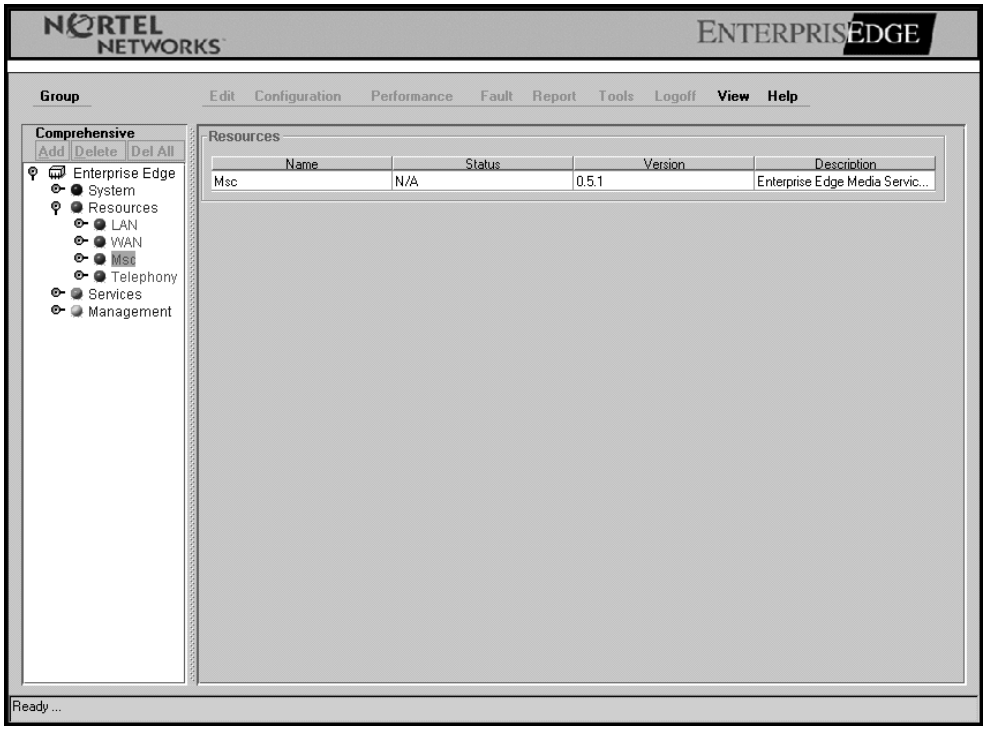
The WAN Access Parameters are:

Setting	Definition
Authentication	Lets users specify the authentication type for the link. Users can choose AllowClearText or EncryptedOnly. If EncryptedOnly is selected, only encrypted authentication such as CHAP is used on this interface during PPP authentication protocol. If AllowClearText is selected, CHAP is used first and if the receiving end of the link declines, PAP is used to authenticate the link user.
Two Way Authentication	Lets users enable or disable link authentication in both directions.
User ID (name password)	Lets users specify a user name and a password that the link uses to authenticate itself while dialing out to another router.

1. Scroll to find the WAN Access Parameters.
2. From the **Authentication** list box select the authentication type.
3. From the **Two Way Authentication** list box select the two-way authentication type.
4. In the **User ID (name password)** box type the user ID, separating the user name and password with a space.
5. Press the **Tab** key to save the settings.
6. Click the **WAN** navigation key to close the navigation tree.

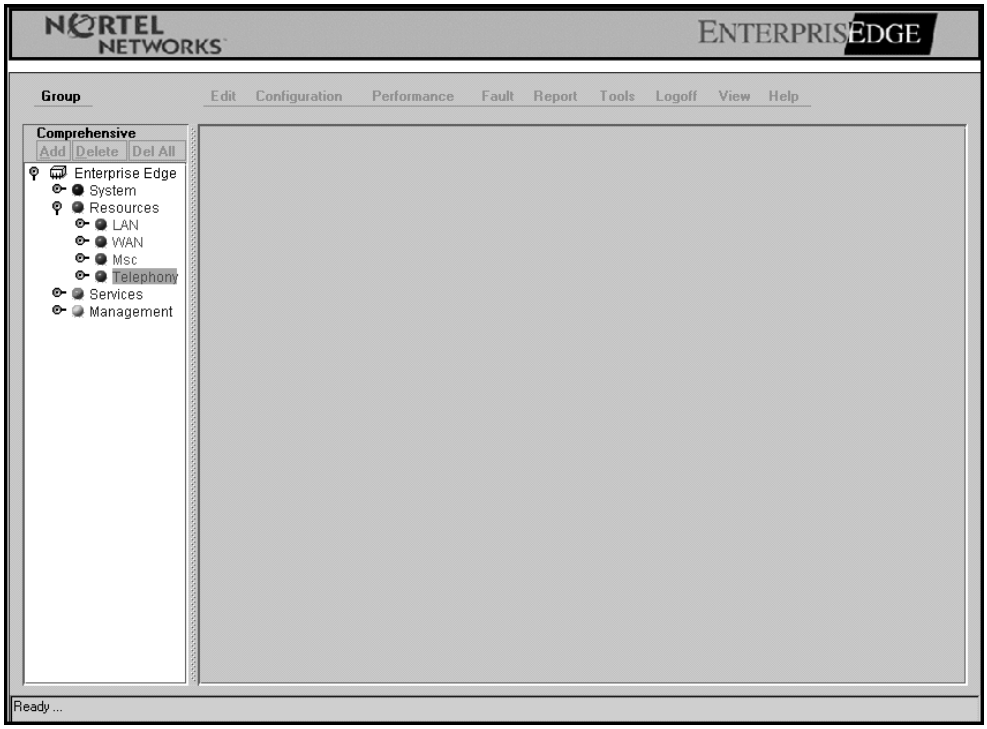
MSC

1. On the Navigation Tree click **MSC** to view the available MSC resources to configure.
   The MSC Resources screen appears.



Telephony

1. On the Navigation Tree click **Telephony** to view the available telephony resources to configure.
   The Telephony Resources screen appears.



2. Click the **Resources** navigation key to close the navigation tree.

Configuring Services Settings

6

Configuring Services Settings includes:

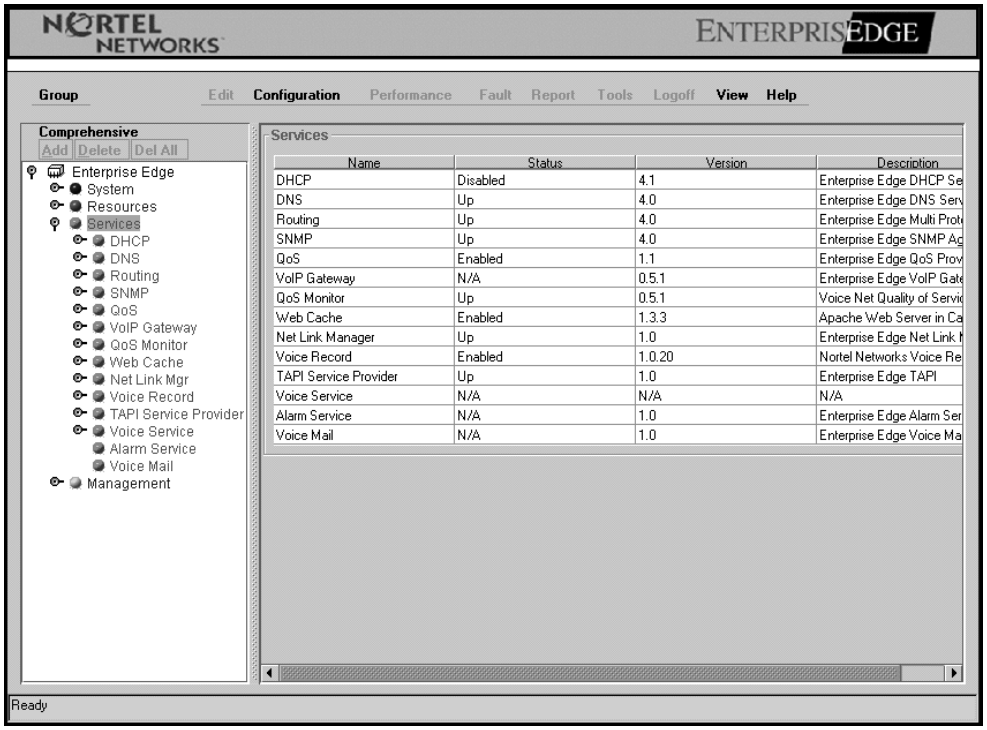
- DHCP Settings
- DNS Settings
- Web Caching/Proxy
- Routing settings

To access the services settings:

1. On the menu click **Group** and then click **Services**
   or
   click **Group** and then click **Comprehensive**.

2. On the navigation tree click the **Enterprise Edge** key and then click the **Services** key.
   The available Enterprise Edge services appear.

3. Click the **Services** navigation key to expand the navigation tree.



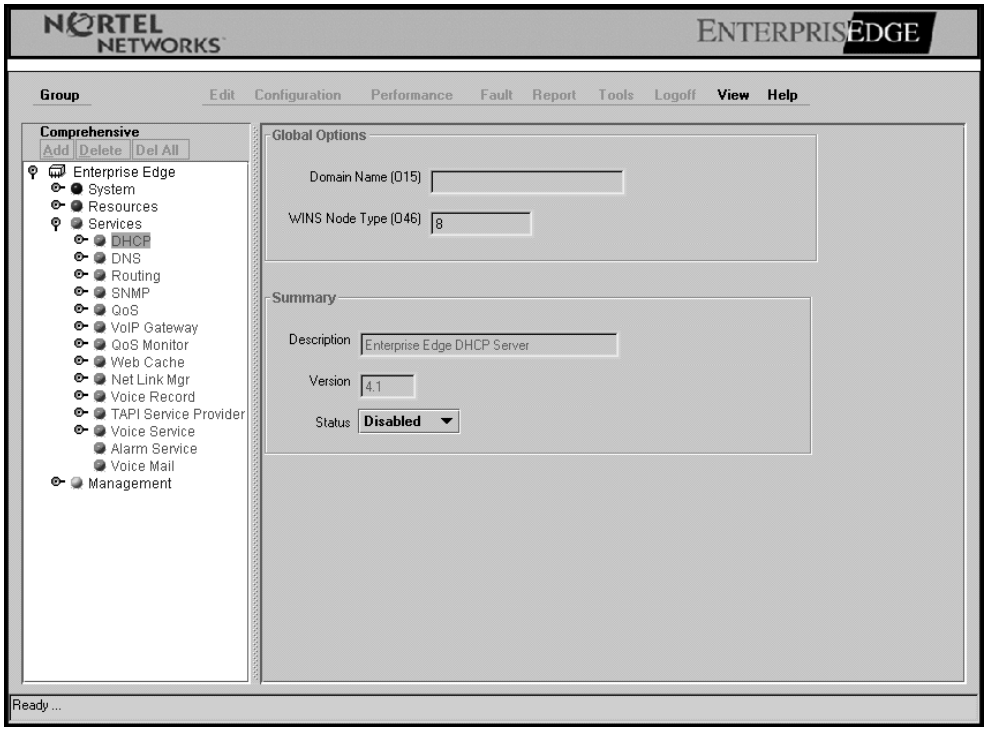
DHCP

To configure DHCP services settings:

1. On the navigation tree click **DHCP** to view the available resources to configure.
   Click the DHCP navigation key to expand the navigation tree, but clicking on the key doesn't display the summary of configurable DHCP services. You must click DHCP.

   The DHCP Global Options and Summary settings appear.

2. Scroll to view any settings not displayed on Unified Manager.



The settings in the DHCP Global Options and DHCP Summary screen are:

Setting	Definition
Domain Name	Lets users specify a domain name that is passed to the client when Enterprise Edge responds to a client's DHCP requests. This setting is automatically set to 'Domain' field in 'DNS Summary' page. This means that all the DHCP clients of an Enterprise Edge server are in the same DNS domain as the Enterprise Edge server. This is also correct since Enterprise Edge runs only a DNS cache and does not introduce another DNS zone. Change the Domain setting in the DNS Summary to make a change in this setting. Occasionally you can change the value of Domain in DHCP. If you do, first make any changes to Domain in the DNS Summary to avoid overwriting your changes.
WINS Node Type	Lets users specify a clients WINS node type. Enterprise Edge automatically sets this value to 8 (indicating H-Node) if the IP Address is changed on any of the LAN interfaces. All DHCP clients of Enterprise Edge are set to h-node type when they get their IP properties from Enterprise Edge. This setting configures the DHCP client PCs to use p-node name resolution before resorting to b-node name resolution, which is efficient when there is a WINS server configured for the network. Enterprise Edge also includes a WINS server. Other options available for this field are: 1: indicates a b-node that uses broadcast mechanism for NetBIOS name resolution 2: indicates a p-node that uses point-to-point mechanism involving a WINS Server for NetBIOS name resolution 4: indicates a m-node that first uses broadcast and then point-to-point mechanism for NetBIOS name resolution.
Description	Shows a description of the Enterprise Edge server.
Version	Shows the version number of the Enterprise Edge server.
Status	Lets users enable or disable the DHCP server. When disabled, clients need to be assigned static IP addresses.

3. In the **Domain Name** box type the appropriate domain name.
   This is set in Enterprise Edge configuration. Use caution if you change it.

4. In the **WINS Node Type** box type the appropriate WINS Node Type.
   This is set in Enterprise Edge configuration. Use caution if you change it.

5. From the **Status** list box select either enable or disable.

6. Press the **Tab** key to save the settings.

DHCP LAN

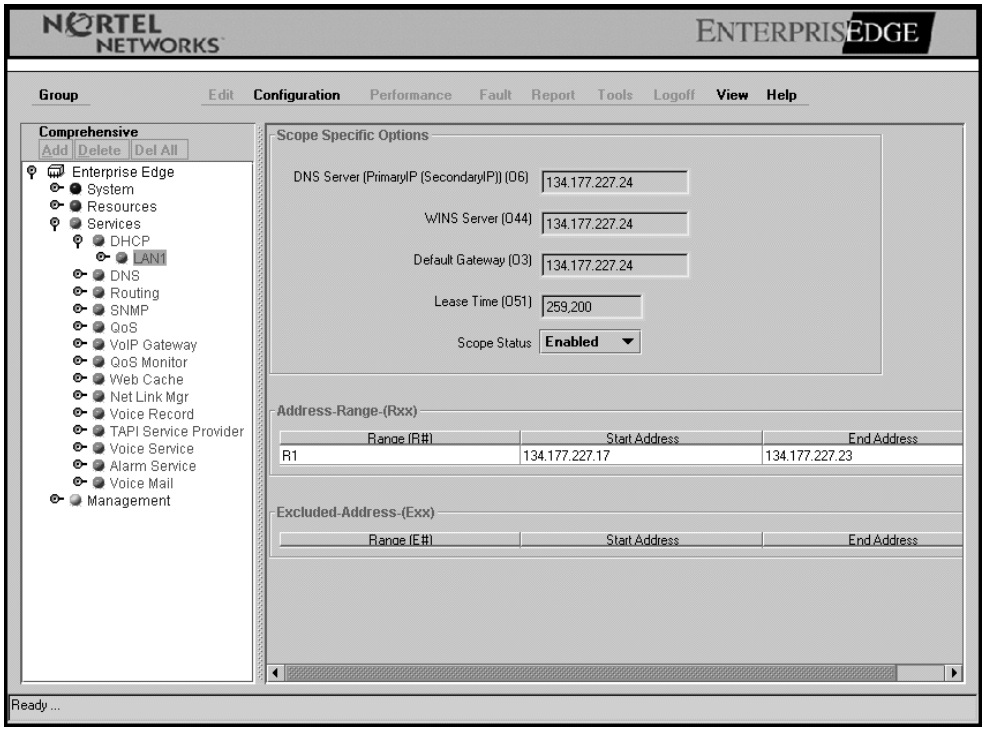
1. Click the **DHCP** navigation key to expand the navigation tree.

2. On the Navigation tree click **LAN1**.
   Clicking the LAN1 navigation key causes the key to disappear. You must choose LAN1 to display the configurable DHCP LAN1 services. If your Enterprise Edge system has multiple LAN interfaces, if is possible that you see multiple DHCP Scopes under DHCP. They are be named LAN1, LAN2. This section describes configuring DHCP scope for LAN1. Follow the same instructions to configure any of the parameters under scope for LAN2.

   The screen displays the LAN Scope Specific Options, Address Range, and Excluded Address Range dialog box.

3. Scroll to view settings not displayed on Unified Manager.

4. You configure the scope-specific options dialog box from Unified Manager. The LAN address range and the LAN excluded address services screen is configured through the menu.



Note: If the IP Address or subnet mask for a LAN interface is changed, the corresponding DHCP scope is created or modified for the interface. This operation also involves setting default values for some parameters. By default, Enterprise Edge sets the IP Address of corresponding LAN interface to DNS Server, WINS Server, Default Gateway options of the scope. It also sets the lease time to 3 days, creates a range of addresses for the scope. If the IP Address of the LAN interface is in the lower half of the subnet, the address range set for the scope includes all the address above the LAN interface address. If the IP Address of the LAN interface is in the upper half of the subnet, the address range set for the scope includes all the address below the LAN interface address. By default, the scope is enabled.

The DHCP LAN1 Scope Specific Options, Address Range and Excluded Address Range settings are:

Setting	Definition
DNS Server	Lets users specify the clients' DNS server. The value for this parameter is automatically assigned by Enterprise Edge's auto-configuration system. If the IP Address or subnet mask for the corresponding LAN interface is changed, this value gets overwritten. Use caution when changing this value.
WINS Server	Lets users specify the client's WINS server. The value for this parameter is automatically assigned by Enterprise Edge's auto-configuration system. If the IP Address or subnet mask for the corresponding LAN interface is changed, this value gets overwritten. Use caution when changing this value.
Default Gateway	Lets users specify the client's default next-hop router. The value for this parameter is automatically assigned by Enterprise Edge's auto-configuration system. If the IP Address or subnet mask for the corresponding LAN interface is changed, this value gets overwritten. Use caution when changing this value.
Lease Time	Lets users specify the time, in seconds, from an address assignment until the client's lease expires.
Scope Status	Lets users enable or disable the scope.
Address Range	Lets users specify the valid IP addresses that are assigned to DHCP clients.
Excluded Address	Lets users specify IP addresses that are not available to DHCP clients.

To modify the configuration of the Scope Specific Options screen:

1. In the **DNS Server** box type the name of the DNS server.
   This field is configured automatically. Use caution when you change it.

2. In the **WINS Server** box type the name of the WINS server.
   This field is configured automatically. Use caution when you change it.

3. In the **Default Gateway** box type the default gateway.
   This field is configured automatically. Use caution when you change it.

4. In the **Lease Time** box type the lease time.
   This field is configured automatically. Use caution when you change it.

5. From the **Scope Status** list box select the scope status.

6. Press the **TAB** key to save the settings.

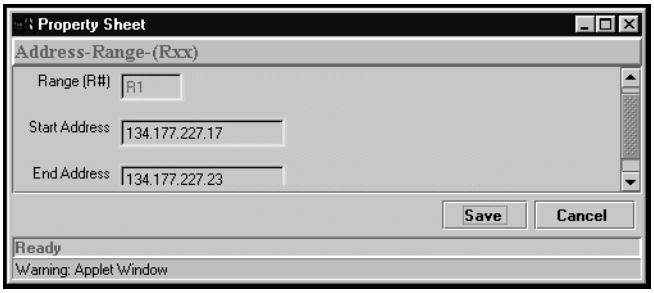
To modify, add, or delete a DHCP address range or excluded address range:

1. Assign only one IP Address range for a DHCP Scope and exclude ranges of addresses in it from being assigned to clients.

To modify address ranges:

1. Click an address in the address range table.

2. On the menu click **Configuration** and then click **Modify Address Ranges**.
   The Address Range dialog box appears.



3. Type the necessary changes in any of the boxes.

4. Click the **Save** button to return to Unified Manager.

To add an address range:

1. On the menu click **Configuration** and then click **Add Address Range**.
   The Address Range dialog box appears.

2. In the **Range** box type the range.
   The range field uniquely identifies a range value in the scope. The value for this field is used as key, and must follow certain conventions. It must always start with the prefix 'R' followed by a unique number identifying the range in the table. For example, 'R2' is a valid name.While adding, specify non-recurring values for the unique number. While adding, if you specify an existing range name, it modifies the existing range. Using non-sequential numbers results in automatic reassignment of sequential numbers. When you modify a range, you can't change the range name. The range name does not have any significance other than identifying an entry.

3. In the **Start Address** box type the start address.

4. In the **End Address** box type the end address.
   Scroll to see any fields that are not displayed.
   Make sure the start address and end address are in the same subnet.

5. Click the **Save** button to return to Unified Manager.

To delete address ranges:

1. Click an address in the **Address Range** table.

2. On the menu click **Configuration** and then click **Delete Address Ranges**.
   A message appears asking you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

   Note: Deleting or modifying an IP Address range removes any excluded addresses that are completely contained in the original address range value.

To modify excluded address ranges:

1. Click an excluded address in the **Excluded Address Range** table.

2. On the menu click **Configuration** and then click **Modify Excluded Address Ranges**.
   The Excluded Address Range dialog box appears.

3. In any box that requires modification type the necessary changes.

4. Click the **Save** button to return to Unified Manager.

To add excluded address ranges:

1. On the menu click **Configuration** and then click **Add Excluded Address Range**.
   The Excluded Address Range dialog box appears.

2. In the **Range** box type the range.

   Note: The range field uniquely identifies an excluded range value in the scope. The value for this field is used as key, and must follow certain conventions. It must always start with the prefix 'E' followed by a unique number identifying the range in the table. For example, 'E2' is a valid name. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing excluded range name, it modifies the existing range. Using non-sequential numbers results in automatic reassignment of sequential numbers. When you modify an excluded range, you can't change the range name. The excluded range name does not have any significance, other than uniquely identifying an entry.

3. In the **Start Address** box type the start address.

4. In on the **End Address** box type the end address.
   Scroll to see any fields that are not displayed.

   Note: Make sure the start address and end address are in the same subnet, and an excluded address range is completely contained in an IP address range specified for the subnet.

5. Click the **Save** button to return to Unified Manager.

To delete excluded address ranges:

1. Click an excluded address in the **Excluded Address Range** table.

2. On the menu click **Configuration** and then click **Delete Excluded Address Ranges**.
   A message appears that asks you to confirm the deletion.

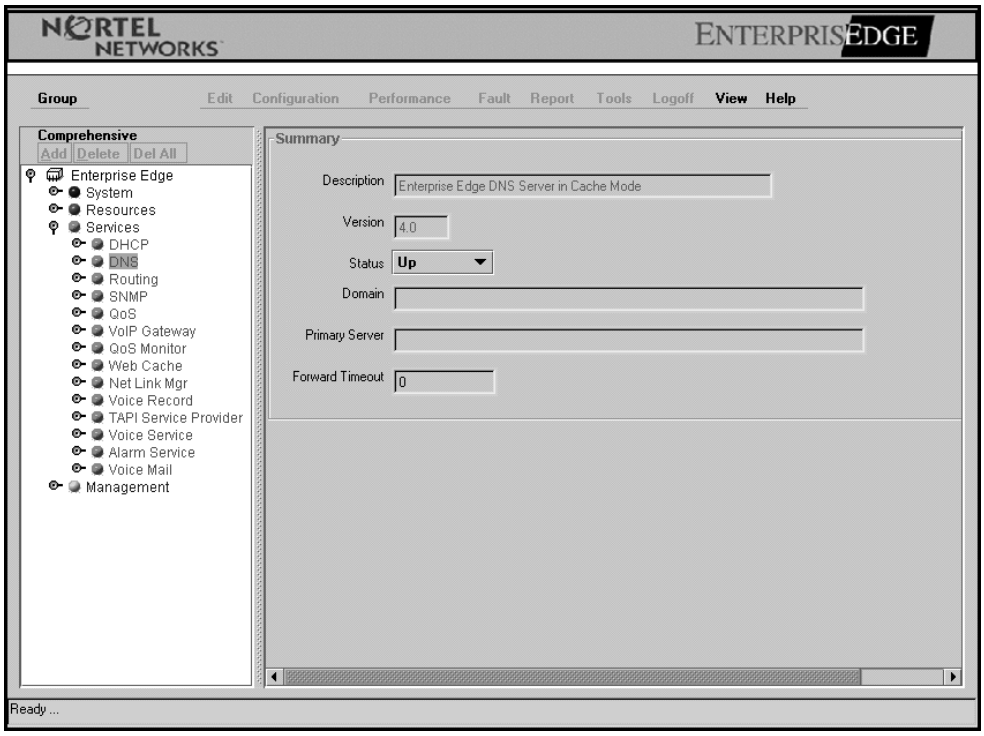
3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

4. Click the **DHCP** navigation key to close the navigation tree.

DNS

To configure DNS services settings:

1. On the navigation tree click **DNS**.
   Clicking the DNS navigation key causes the key to disappear. You must click DNS to view the available configurable DNS services.
   The DNS Summary screen appears.



The DNS Summary settings are:

Setting	Definition
Description	Lets users view the description of the server in cache mode.
Version	Lets users view the version of the software interface.
Status	Lets users enable or disable the DNS cache proxy in Enterprise Edge.
Domain	Lets users specify the domain name that Enterprise Edge and its DHCP clients uses. When modified, contents of this setting are automatically copied to Domain Name global options (O15) under DHCP.
Primary Server	Lets users specify the primary server IP address in a valid dot format. More than one address can be specified separated by a space; DNS cache uses them in the specified order to resolve names.
Forward Timeout	Lets users specify the time-out, in seconds, used in resolving queries using the DNS servers that are specified in DNS server.

To modify the configuration of the DNS summary:

2. From the **Status** list box select the status.

3. In the **Domain** box type the domain.

4. In the **Primary Server** box type the primary server.

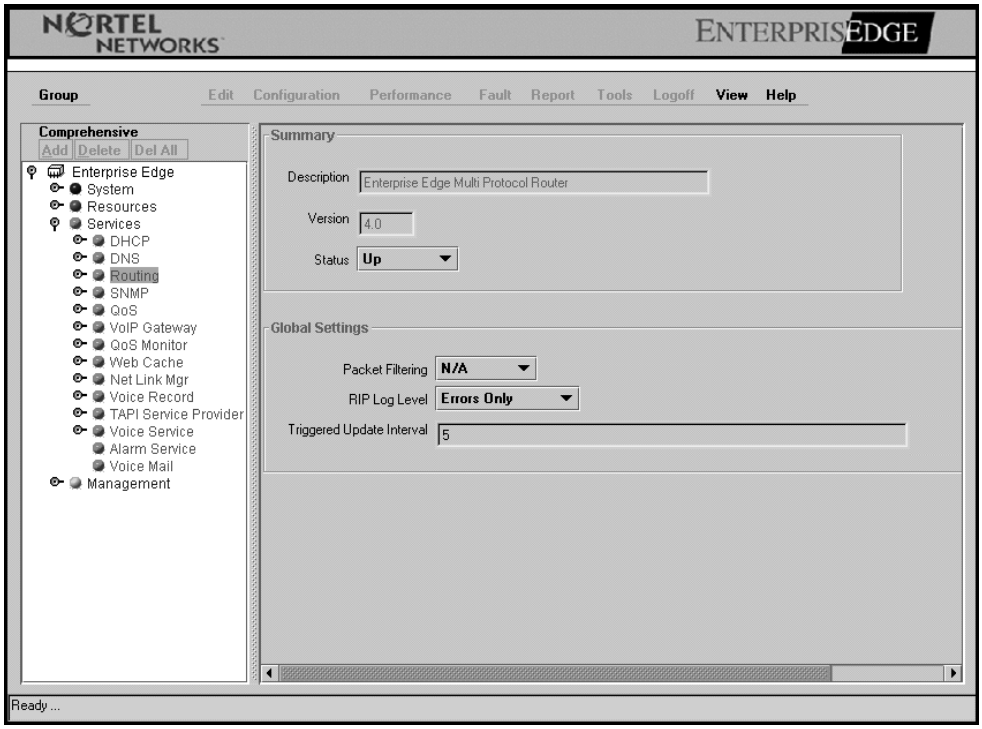
5. In the **Forward Timeout** box type the forward timeout.

6. Press the **Tab** key to save the settings.

Routing

To configure routing services settings:

1. On the Navigation Tree click **Routing** to view the services to configure. Clicking the Routing navigation key expands the navigation tree but doesn't display the summary of configurable routing services. You must click Routing.
   The Summary and Global Settings screen appears.



The LAN1 Summary and RIP Parameters Routing settings are:

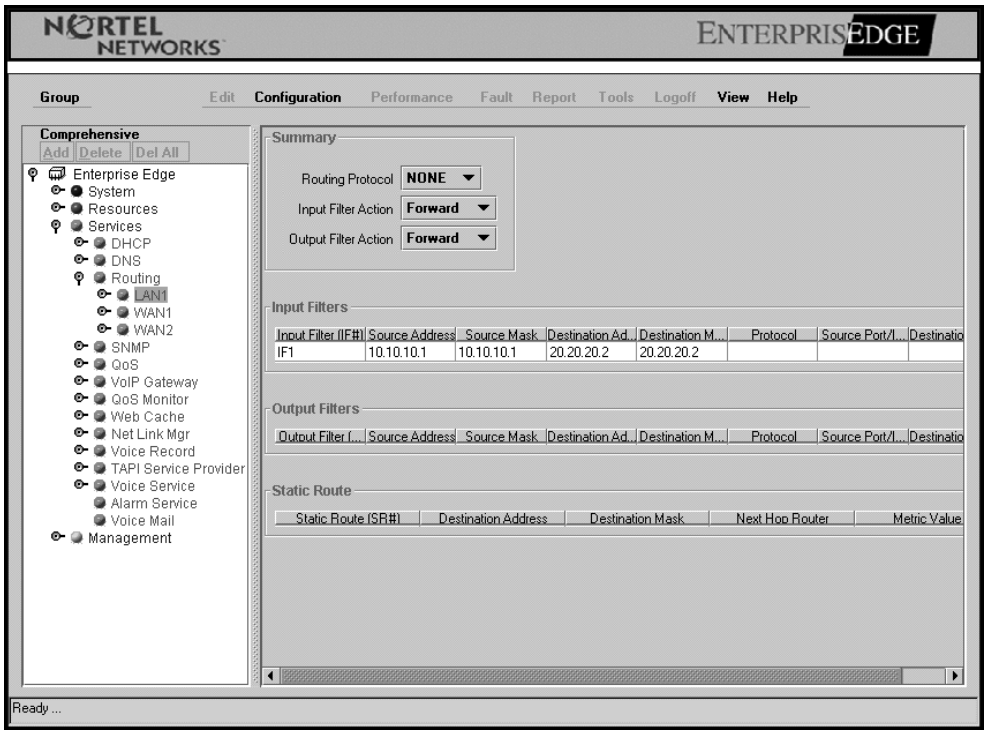
Settings	Definition
Description	Shows a description of the router.
Version	Shows the version of the router.
Status	Lets users enable or disable the router.
Packet Filtering	Lets users enable or disable packet filtering. When the system comes up the first time, this value is N/A, indicating that the Management system cannot retrieve pertinent information. Set it to Disabled or Enabled and valid values are displayed. Disabling packet filtering here disables it on all interfaces. The router performs better when packet capturing is disabled.
RIP Log Level	Lets users specify a log-level for the RIP routing protocol manager: maximum generates the maximum log warnings also, generates a log for warning conditions too errors only, generates log errors only (for use during normal operations) disabled disables logging (not recommended).
Triggered Update Interval	Lets users specify the minimum interval between sending triggered updates.

1. From the **Status** list box enable or disable the router.
2. From the **Packet Filtering** list box enable or disable packet filtering.
3. From the **RIP Log Level** list box select the RIP log level.
4. In the **Triggered Update Interval** box type the triggered update interval.
5. Press the **TAB** key to save the settings.

LAN Routing

This section describes the instructions to configure LAN1 interfaces for routing. If there are other existing LAN or WAN interfaces, they also appear in Routing. Follow the same instructions to configure them.

1. On the navigation tree click the **Routing** navigation key to expand the menu.
2. On the navigation tree click **LAN1**.
   Clicking the LAN1 navigation key causes the key to disappear. You must click LAN1 to view the available services to configure.
   The Summary, Input Filter, Output Filter, and Static Route screen appears.



Note: The RIP Parameters screen is not displayed unless you choose RIP as your routing protocol in the LAN1 summary screen. To display the RIP parameters, click the **Routing Protocol** list box and choose RIP. Then press the **Tab** key to update the screen. A configurable RIP screen appears.

You configure the Routing summary screen from Unified Manager.

The Input Filter, Output Filter, and Static Route screen is configured through the menu.

The LAN1 Routing Services Summary and RIP Parameters settings are:

Setting	Definition
Routing Protocol	Lets users select the Routing protocol to run over the interface. Select RIP to run RIP protocol or select NONE to disable running any routing protocol. If RIP is selected, interface-specific RIP parameters appear in the bottom of the screen. You can configure other RIP parameters on this interface
Input Filter Action	Determines what action is performed for the packets that match the filter criteria. You can either forward them to upper layer, possibly for further routing or drop them. You can select the action only if you have set any of the input or output filters. Otherwise, they show up as N/A and you can't modify them.
Output Filter Action	Determines what action is performed for the packets that match the filter criteria. You can either forward them to the next hop or drop them. You can select the action only if you have set any of the input or output filters. Otherwise, they show up as N/A and you can't modify them.
Metric	Specifies the associated metric value for the routes through this interface. Metric values of all routes learned through this interface are incremented by this value. The final value used in making routing decisions is forwarded to other routes through RIP updates.
Routing Table Update Mode	Lets users specify the routing table update mode for the interface. In On Demand mode, the router sends its table when requested by another established router. In Periodic mode, the router sends its table to other established router at regular intervals.
Route Announcement Type	Lets users specify the route-announcement type for the specified interface. The choices are: Disabled: sending RIP packets is disabled on this interface. This requires the other routers in the subnet have static routes configured to access the Enterprise Edge server. RIP 1: sends RIP v1 packets in broadcast only. RIP 1 Compatible: sends RIP v1 and RIP v2 packets in broadcast. Use this for a mixed environment of RIP v1 and RIP v2 RIP 2: sends RIP v2 packets in multicast only. Use this only if all other routers connected to the Enterprise Edge server are RIP v2 capable.
Route Accept Type	Lets users choose to accept announcements in either RIP1, RIP2, or both formats. The choices are: Disabled: accepting RIP packets is disabled. If this choice is selected, the user is prompted to create static routing entries in the Enterprise Edge server to access other networks connected through this interface. This method is preferable if you want to keep the routing table small in the Enterprise Edge server. RIP 1: accepts only RIP v1 packets RIP 1 Compatible: accepts packets of both RIP v1 and RIP v2 RIP 2: accepts only RIP v2 packets.
Route Expiration Interval	Lets users specify, in seconds, the time interval to mark an established router that has not updated its table eligible for removal.
Route Removal Interval	Lets users specify, in seconds, the time interval between route expires and when it is removed from the routing table.

Setting	Definition
Route Announcement Interval	Lets users specify, in seconds, the time interval between route announcements.
Route Tag	Lets users create a special tag that is included in routes announced over the interface. This helps identify route packets while debugging routing problems using a network sniffer.
Poisoned Reverse	Lets users enable poison reverse. The choices are: Actual: the actual, original RIP updates are performed over this interface. All the routes learned through this interface are also included as is in the RIP updates sent over this interface. This leads to mutually deceiving route updates that require multiple routing updates that is termed 'counting to infinity' in RIP terms. Split: in the routing updates sent over this interface, router does not include the routes learned over this interface. This mode performs better than Actual, but still requires significant amount of time to converge routes. It requires all routes corresponding to an unreachable network expire before removing them from the routing table Poison Reverse: in the routing updates sent over this interface, the router includes the routes learned over this interface, but 'poisoned metrics'. All metric values are set to RIP infinity (16) for the routes learned through this interface. This results in the fastest convergence.
Triggered Updates	Lets users enable triggered updates, or immediate route update announcements whenever a metric or other parameter changes in the route table entries. If triggered updates are enabled, the changes are gathered for the interval specified in the global parameter Triggered Update Interval and then sent over this interface. Triggered updates results in more frequent, smaller RIP updates.
Announce Default Route	Lets users enable or disable announcing default routes in incoming route announcements. Use caution when enabling this feature as improper configuration causes a loss of network connectivity. Default routes are always set statically on the router.
Accept Default Route	Lets users enable or disable accepting incoming default routes. Set default routes as static routes. If you are run Net Link Manager to automatically backup primary WAN link using a dial-up link, it manages the default routes and the default routes that you add are non-operational as soon as a link breaks or comes up.

To modify the configuration of the LAN1 routing summary screen:

1. From the **Routing Protocol** list box select **NONE** or **RIP**.
   If you choose RIP, press the **Tab** key to update the screen.
   A configurable RIP Parameters screen appears.

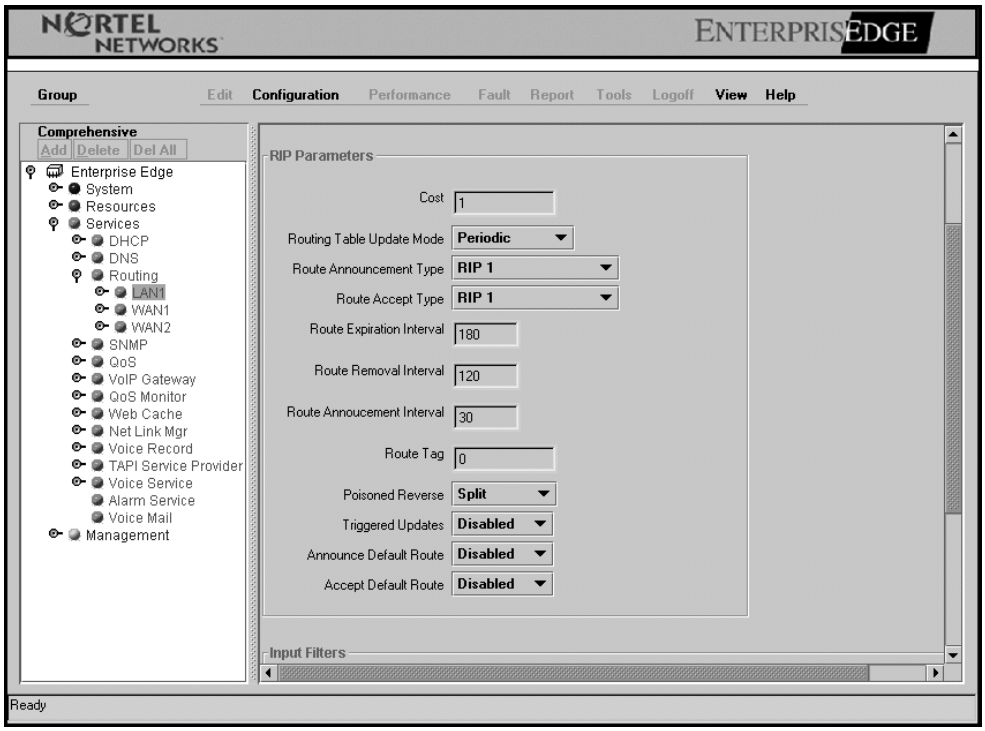
2. From the **Input Filter Action** list box select the input filter action.

3. From the **Output Filter Action** list box select the output filter action.

4. Press the **Tab** key to save the settings.
   This operation fails if filters have not been added to the interface.

To modify the configuration of the RIP Parameters:

1. Scroll to locate the RIP Parameters screen.



2. In the **Metric** box type the cost integer value.

3. From the **Routing Table Update Mode** list box select the mode.

4. From the **Route Announcement Type** list box select the routing announcement.

5. From the **Route Accept Type** list box select the route accept type.

6. In the **Route Expiration Interval** box type the expiration interval value in seconds.

7. In the **Route Removal Interval** box type the removal interval value in seconds.

8. In the **Route Announcement Interval** box type the announcement interval value in seconds.

9. In the **Route Tag** box type the route tag.

10. From the **Poisoned Reverse** list box select the appropriate mode.

11. From the **Triggered Updates** list box enable or disable triggered updates.

12. From the **Announce Default Route** list box enable or disable announcing default routes.

13. From the **Accept Default Route** list box enable or disable accepting default routes.

14. Press the **TAB** key to save the settings.

The LAN1 Filter and Static Route settings are:

Setting	Definition
Input filter	Specifies the filter name and identifies an individual input filter on the specified interface. Its value must follow certain conventions. It must have the prefix IF followed by a unique number that identifies the input filter on the interface. For example, IF2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing filter name, it modifies the existing filter. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a filter, you can't change the name. The filter name does not have any significance other than to identify an entry.
Output filter	Specifies the filter name and uniquely identifies an individual output filter on the specified interface. Its value must follow certain conventions. It must have the prefix OF followed by a unique number that identifies the input filter on the interface. For example, OF2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing filter name, it modifies the existing filter. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a filter, you can't change the name. The filter name does not have any significance other than to identify an entry.
Source address	Lets users specify the source IP address in a valid dot format. If you don't want to match the source address field in your filter, leave this setting and the source mask empty.
Source mask	Lets users specify the source mask for the IP address in a valid dot format. If you specify a source address, you must specify the source mask. If you don’t specify the source address, you must not specify the source mask. The source address and source mask must match. Bitwise, the source address and the source mask must be equal to the source address.
Destination address	Lets users specify the destination IP address in a valid dot format. If you are specifying a filter, this field specifies the destination address of the IP packet that matches the filter. If you don't want to match the destination address, leave this field empty. If you are specifying a static route, this field must not be empty. It must be a valid network or host address.The destination mask must match the address specified in this setting.
Destination mask	Lets users specify the mask of the destination address in a valid dot format. If you specify a destination address, you must specify a destination mask. If you don’t specify the destination address, you must not specify the source mask. The destination address and destination mask must match; i.e. bitwise AND of destination address and destination mask should be equal to destination address.

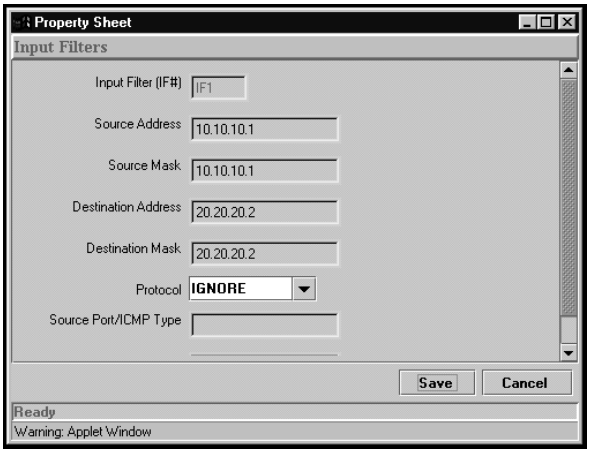
Setting	Definition
Protocol	Lets users specify the protocol to match the filter. The choices are: TCP: look for the TCP protocol packets. You can specify source and destination service ports in other fields. If you don't specify any port numbers all packets that match this protocol and other criteria, if any, match the filter. UDP: look for UDP protocol packets. You can further specify source and destination service ports in other fields. If you don't specify any port numbers all packets that match this protocol and other criteria, if any, match the filter. ICMP: look for ICMP protocol packets. You can further specify the ICMP message types and ICMP codes in other fields. If you don't specify any ICMP types or codes all packets that match this protocol and other criteria, if any, match the filter.
Source port/ ICMP type	If the protocol chosen is UDP or TCP, this lets users specify the source port to match the filter. If the protocol chosen is ICMP, this field specifies the ICMP code value to look for in the packet to match the filter. Destination Port/ICMP Code: If the protocol chosen is UDP or TCP, this lets users specify the additional destination service port to match the filter. If the protocol chosen is ICMP, this field can contain the optional ICMP code.
Static Route	Specifies the static route name and is used as a key to uniquely identify an individual static route on the specified interface. Its value must follow certain conventions. It must have the prefix SR followed by a unique number that identifies this static route on this interface. For example, SR2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing static route name, it modifies the existing static route. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a static route, you can't change the name. The static route name does not have any significance other than to identify an entry.
Next Hop Router	Lets users specify the IP address in a valid dot format for the next hop router.
Metric Value	Lets users specify the metric value associated with the interface. The metric is added to the hop count of the routes received through the interface.

Note: If input and output filters are not defined for the LAN1 interface, modifying input filter action or output filter action in the summary causes an error message.

To modify the configuration of LAN1 input filters:

1. Click an **input filter** in the input filter table.

2. On the menu click **Configuration** and then click **Modify Input Filter**. The Input Filters dialog box appears.



1. In the **Source Address** box type the source address.

2. In the **Source Mask** box type the source mask.

3. In the **Destination Address** box type the destination address.

4. In the **Destination Mask** box type the destination mask.

5. From the **Protocol** list box select the response.

6. In the **Source Port/ICMP Type** box type the source port/ICMP type.

7. In the **Destination Port/ICMP Type** box type the destination port/ICMP type.

8. Click the **Save** button to return to Unified Manager.

To add LAN1 input filters:

1. On the menu, click **Configuration** and then click **Add Input Filter**. The Input Filter dialog box appears.
2. In the **Input Filter** box type the input filter.
3. In the **Source Address** box type the source address.
4. In the **Source Mask** box type the source mask.
5. In the **Destination Address** box type the destination address.
6. In the **Destination Mask** box type the destination mask.
7. From the **Protocol** list box select the response.
8. In the **Source Port/ICMP Type** box type the source port/ICMP type.
9. In the **Destination Port/ICMP Type** box type the destination port/ICMP type.
10. Click the **Save** button to return to Unified Manager.

To delete LAN1 input filters:

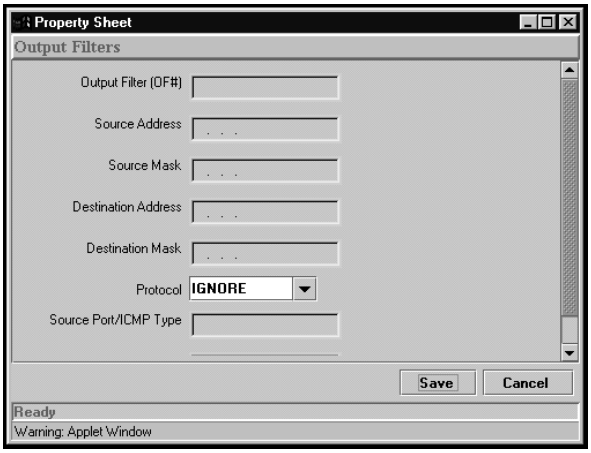
1. Click a filter in the **Filter** table.
2. On the menu, click **Configuration** and then click **Delete Input Filter**. A message appears that asks you to confirm the deletion.
3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

To modify the configuration of LAN1 output filters:

1. Click an output filter in the **Output Filter** table.
2. On the menu, click **Configuration** and then click **Modify Output Filter**.
3. Follow the steps for modifying input filters.

To add LAN1 output filters:

1. On the menu, click **Configuration** and then click **Add Output Filter**. The Output Filter dialog box appears.



2. In the **Output Filter** box type the output filter.
3. In the **Source Address** box type the source address.
4. In the **Source Mask** box type the source mask.
5. In the **Destination Address** box type the destination address.
6. In the **Destination Mask** box type the destination mask.
7. From the **Protocol** list box select the response.
8. In the **Source Port/ICMP type** box type the source port/ICMP type.
9. In the **Destination Port/ICMP type** box type the destination port/ICMP type.
10. Click the **Save** button to return to Unified Manager.

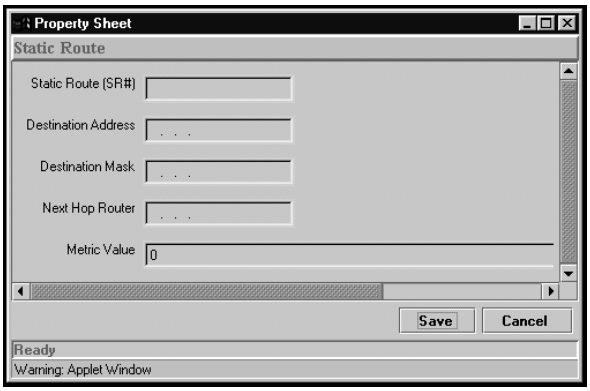
To delete LAN output filters:

1. Click on an output filter in the **Output Filter** table.
2. On the menu, click **Configuration** and then click **Delete Output Filter**.
3. Follow the steps for deleting input filters.

To modify the configuration of static routes:

1. Click a static route in the **Static Route** table.

2. On the menu, click **Configuration** and then click **Modify Static Route**. The Static Route dialog box appears.



3. In the **Destination Address** box type the destination address.

4. In the **Destination Mask** box type the destination mask.

5. In the **Next Hop Router** box type the next hop router.

6. In the **Metric Value** box type the metric value.

7. Click the **Save** button to return to Unified Manager.

To add LAN1 static routes:

1. On the menu, click **Configuration** and then click **Add Static Route**. The Static Route dialog box appears.

2. In the **Static Route** box type the static route.

3. In the **Destination Address** box type the destination address.

4. In the **Destination Mask** box type the destination mask.

5. In the **Next Hop Router** box type the next hop router.

6. In the **Metric Value** box type the appropriate metric value.

7. Click the **Save** button to return to Unified Manager.

To delete LAN static routes:

1. Click a static route in the **Static Route** table.

2. On the menu, click **Configuration** and then click **Delete Static Route**.

3. Follow the steps for deleting output filters.

WAN Routing

To configure WAN routing services:

1. Click the **Routing** navigation key to expand the navigation tree.

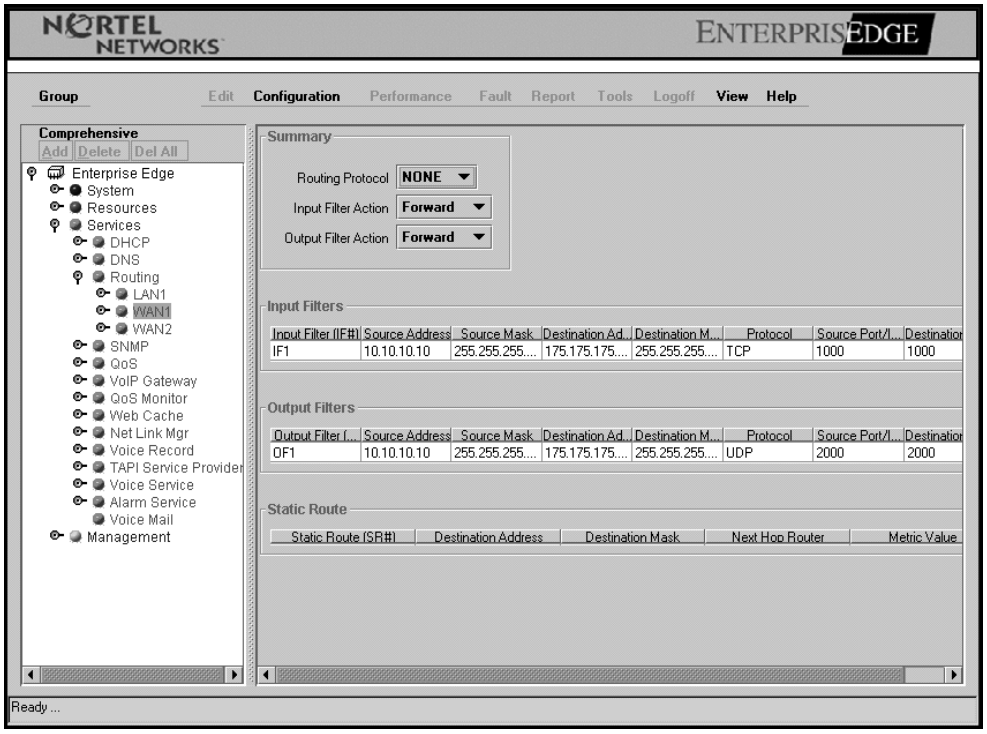
2. On the navigation tree, click **WAN1** or **WAN2**.
   Clicking the WAN1 or WAN2 navigation key causes the key to disappear. You must click WAN1 or WAN2 to view the configurable WAN resources.

   The Summary, RIP Parameters, Input Filter, Output Filter, and Static Route screen appears.

   Note: The RIP Parameters screen is not displayed unless RIP is chosen as your routing protocol in the WAN summary screen. To display the RIP parameters, click the **Routing Protocol** list box and select RIP. Then press the **Tab** key to update the screen. A configurable RIP screen appears.

3. Use the scroll bars to locate any fields that are not displayed.

4. Configure the WAN1 or WAN2 routing summary and RIP Parameters screen from Unified Manager.
   Configure the input Filter, output filter, and static route dialog box from the menu.



5. Follow the steps outlined in LAN routing settings to complete your configuration process.

6. Clicking the **Routing** navigation key to close the navigation tree.

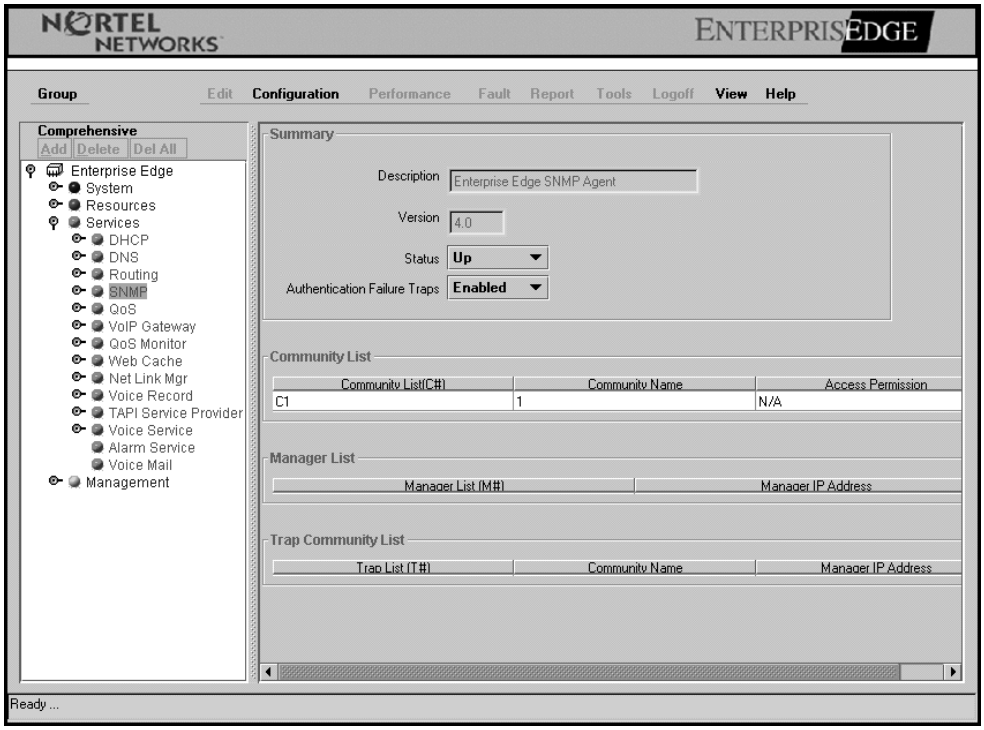
SNMP

To configure SNMP services settings:

1. On the navigation tree click **SNMP**.
   Clicking the SNMP navigation key causes the key to disappear. You must click SNMP.

   The screen displays the SNMP Summary, Community List, Manager List, and Trap Community List screen.

2. Configure SNMP summary screen from Unified Manager.
   Configure the SNMP Community List, Manager List, and Trap Community List from the menu.



The SNMP settings are:

Setting	Definition
Description	Shows the description of the SNMP agent.
Version	Shows the version of the SNMP agent
Status	Lets users enable or disable the SNMP agent.
Authentication Failure Traps	Lets users enable or disable authentication failure traps. When enabled, the SNMP agent sends authentication failure traps if there is an authentication failure. Authentication failure happens if an SNMP manager application provides a wrong community string or performs an operation that is not permitted for a community.

3. From the **Status** list box select **enable** or **disable**.

4. From the **Authentication Failure Traps** list box select **enable** or **disable**.

5. Press the **Tab** key to save the changes.

SNMP Community List, Manager List, and Trap Community List

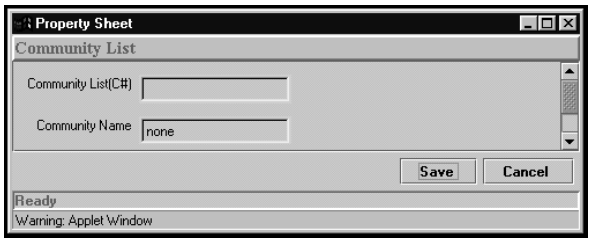
The SNMP community list, manager list and trap community services settings are:

Setting	Definition
Community List	Lets users specify the entry name used as a key to uniquely identify an individual community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix C followed by a unique number that identifies the community name entry on the agent. For example, C2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing community entry name, it modifies the existing community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a community entry, you can't change the name. The community entry name does not have any significance other than to identify an entry.
Community Name	Lets users specify the name of the community that the individual managers use to interact with this agent. When creating community entries, various access permissions are associated with these names. Manager stations that use different community names get different permissions on the SNMP agent. While creating trap communities, various manager IP addresses are associated with these values. All the manager stations in a trap community get traps with the community name specified in the entry.
Manager List	Lets users specify the entry name used to identify an individual manager entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix M followed by a unique number that identifies the manager entry on the agent. For example, M2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing manager entry name, it modifies the existing manager entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a manager entry, you can't change the name. The manager entry name does not have any significance, other than to uniquely identify an entry.
Manager IP address	Lets users specify the IP Address of the SNMP Manager station corresponding to this entry. If no manager entries are created, the Enterprise Edge device accepts SNMP requests from all stations. If there is a list of manager entries, Enterprise Edge server accepts SNMP requests from the IP Addresses specified in the list.
Trap List	Lets users specify the entry name used to identify an individual trap community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix T followed by a unique number that identifies the trap community entry on the agent. For example, T2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing trap community entry name, it modifies the existing trap community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a trap community entry, you can't change the name. The trap community entry name does not have any significance, other than to uniquely identify an entry.

To modify the configuration of the Community List, Manager List, and Trap Community List:

To add to the community list:

1. On the menu, click **Configuration** and then click **Add Community**. The Community List dialog box appears.



2. Click the **Community List** box type the community list.

3. Click the **Community Name** box type the community name.

4. Scroll to view the **Access Permission** settings.

5. From the **Access Permission** the list box select the Access Permission.

6. Click the **Save** button to return to Unified Manager.

To modify a community:

1. Click a community in the **Community** table.

2. On the menu, click **Configuration** and then click **Modify Community**.The Community List dialog box appears.

3. Click any box that requires modification and type the necessary changes.

4. Click the **Save** button to return to Unified Manager.

To delete a community:

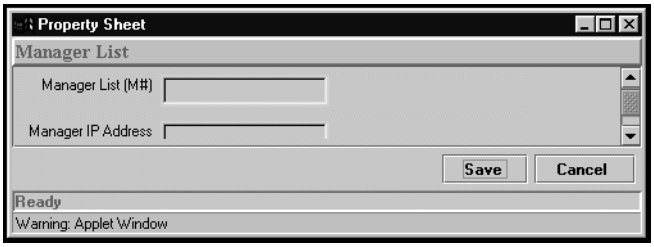
1. Click on a community in the **Community** table.

2. On the menu, click **Configuration** and then click **Delete Community**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

To add a manager:

1. On the menu, click **Configuration** and then click **Add Manager**.
   The Manager List dialog box appears.



2. In the **Manager List** box type the manager list.

3. In the **Manager IP Address** box type the manager IP address.

4. Click the **Save** button to return to Unified Manager.

To modify the manager list:

1. In the **Manager** table, click a manager.

2. On the menu, click **Configuration** and then click **Modify Manager**.
   The Manager List dialog box appears.

3. Click any box that requires modification and type the necessary changes.

4. Click the **Save** button to return to Unified Manager.

To delete a manager:

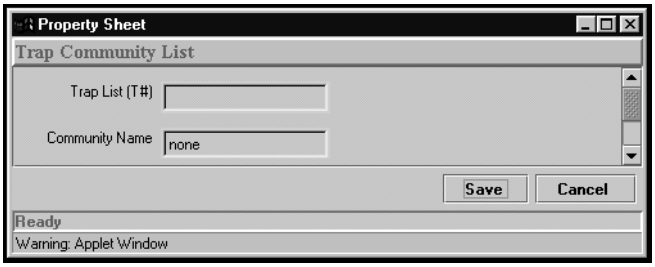
1. In the **Manager** table, click the manager you want to delete.

2. On the menu, click **Configuration** and then click **Delete Manager**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

To add a trap community:

1. On the menu, click **Configuration** and then click **Add Trap Community**.
   The Trap Community List dialog box appears.



2. In the **Trap List** box type the trap list.

3. In the **Community Name** box type the community name.

4. Scroll to see the **Manager IP Address** box.

5. In the Manager IP Address box, type an IP Address for a manager station that is a member of this trap community.

6. Click the **Save** button to return to Unified Manager.

To modify a trap community:

1. In the **Trap Community** table, click the trap community you want to modify.
2. On the menu, click **Configuration** and then click **Modify Trap Community**. The Trap Community List dialog box appears.
3. Click any box that requires modification and type the necessary changes.
4. Click the **Save** button to return to Unified Manager.

To delete a trap community:

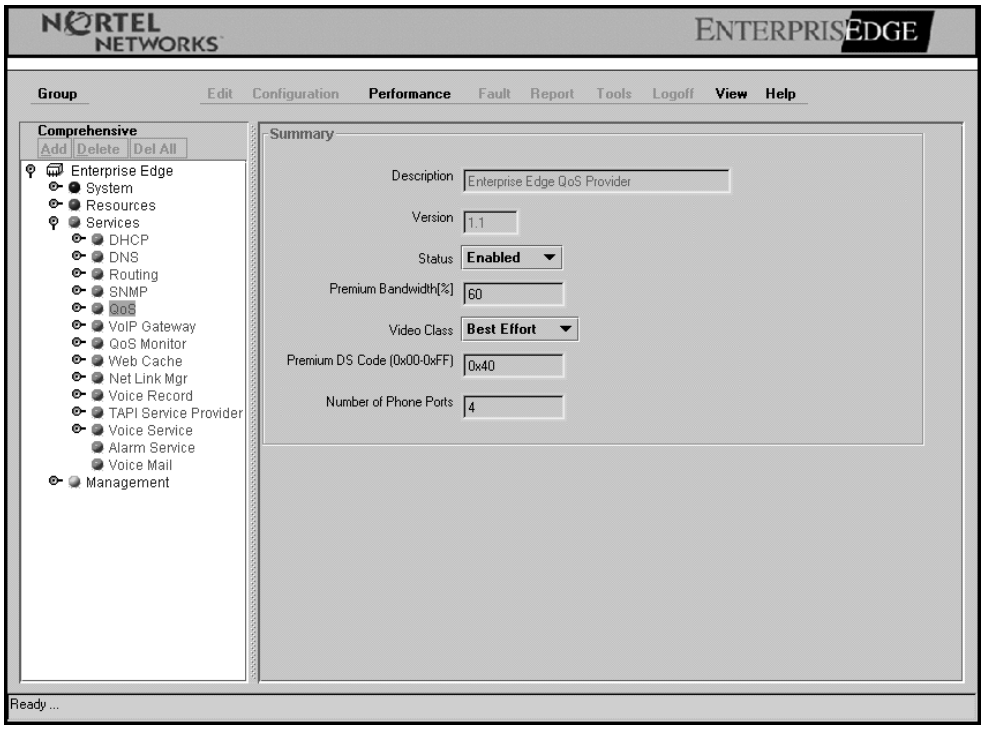
1. In the **Trap Community** table, click the trap community you want to delete.
2. On the menu, click **Configuration** and then click **Delete Trap Community**. A message appears that asks you to confirm the deletion.
3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

QoS

To configure QoS services settings:

1. On the navigation tree click **QoS**.
   Clicking the QoS navigation key expands the navigation tree but doesn't display the summary of configurable QoS services. You must click QoS.

   The QoS Summary screen appears.



The QoS Services Summary settings are:

Setting	Definition
Description	Shows the description of the QoS provider.
Version	Shows the driver version of the QoS provider.
Status	Lets users enable or disable the QoS module.
Premium Bandwidth	Lets users specify, in percentages, the WAN bandwidth reserved for premium traffics. Choose a value for this field based on the link speed, the codecs used by VoIP gateway, the sample rate and the number of concurrent phone calls (from internal VoIP gateway) and other H.323 sessions (like Microsoft NetMeeting traffic) you intend to carry over the WAN link. Refer to WAN overview on page 37 for more information on this topic. Make sure you allocate at least the bandwidth necessary to carry as many phone calls as specified in 'Number of Phone Ports' field below. Otherwise, the QoS provider sees the inconsistent configuration and disables itself when system boots next time, resulting in broken connectivity. Any additional bandwidth that is more than what is required to carry the phone calls is available for other H.323 sessions like NetMeeting sessions from PCs connected to Enterprise Edge box or other data traffic classified as premium, through QoS Filters. This additional bandwidth reserved for premium traffic is always available for other data traffic if there is no additional H.323 traffic or other premium traffic. A network administrator can reserve more WAN bandwidth than that required to carry phone calls and then prevent PC users from using it for NetMeeting sessions by setting filters that drop H.323 traffic at LAN interfaces.
Video Class	Lets users specify the type of priority treatment for video traffic in H223 sessions. The following choices are available: Premium: Video traffic is treated as premium traffic that consumes portions of bandwidth reserved for premium traffic (Premium Bandwidth field). Best Effort: Video traffic is treated as best effort IP traffic that are prioritized among other best-effort traffic passing through the WAN link.
Premium DS Code	Lets users specify the TOS field in the IP header for premium packets. This value is used in conjunction with the frame relay driver in Enterprise Edge's WAN link, if one is being used, as well as rest of the network. If the frame relay is used on WAN link, this code should match the DS Code field in frame relay settings so that frame relay network treats this traffic as high-priority. If rest of the network is diffserv capable, all routers that carry VoIP traffic from theEnterprise Edge server must be configured to treat the traffic with this DS code as high-priority or premium traffic.
Number of Phone Ports	Lets users specify the number of phone ports. This value specifies the number of concurrent phone calls user intends to carry over the WAN interface. QoS Provider layer uses this value to determine how much of the bandwidth reserved for premium traffic is consumed by internal VoIP gateway and how much is left over for other H.323 or other classified premium traffic.
Filter Order	Lets users specify the order that filters are evaluated. If a filter name is listed in filter order, but the actual filter is missing, it is ignored. If an actual filter is omitted from the filter order list, the filter is not effective.

Setting	Definition
Filter	Lets users specify the entry name that is used as a key to uniquely identify an individual filter entry in QoS layer. Its value must follow certain conventions. It must have the prefix F followed by a unique number that identifies this filter. For example, F2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing filter entry name, it modifies the existing filter entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a filter entry, you can't change the name.
Source Address	Lets users specify the source IP address in a valid dot format. If you want to ignore the source address field in filter, leave this field blank. If you specify an address in this field, you should also specify a subnet mask in the Source Mask field.
Source Mask	Lets users specify the source mask of the IP address in a valid dot format. If you specify a source address, you must specify a source mask and vice versa. Make sure that the mask and address match with each other, i.e. bitwise and of mask and address is equal to the address. If you want to specify a range of addresses, use a subnet mask other than 255.255.255.255. For example, address/mask combination 10.10.10.32/ 255.255.255.252 represents addresses 10.10.10.32-10.10.10.35.
Destination Address	Lets users specify a destination IP address in a valid dot format. See the instructions for Source Address.
Destination Mask	Lets users specify a mask for the destination IP address in a valid dot format. See the instructions for Source Mask.
Source Port	Lets users specify a source port to match the filter. Specify a source port only if you choose a TCP or a UDP protocol. If you don't want to include the source port in your filter, select IGNORE for it. Otherwise, select the port for one of the well-known services from the list or type it in the list box. If you type the port, specify the service's numeric port number. You can specify a range of ports by specifying the two limits of the range by a hyphen character, for example, 156-159. You can also specify 0 for the lower limit and 65536 for upper limit.
Destination Port	Lets users specify a destination port to match the filter. It is interpreted the same way as source port.
Protocol	Lets users specify a protocol to match the filter. If you don't want to include a protocol in your filter, select IGNORE for the protocol. Otherwise, select the protocol from the list or type the numeric value of sub-protocol under IP in the box.
PortRange	Lets users reserve and list different UDP port ranges that the Enterprise Edge QoS module uses for VoIP RTP flows. Set the UDP ports to high priority so that VoIP packets are forwarded quickly.
DSCode (TOS) Criteria	Lets users specify the DS Code (TOS) value for the filter to match. Use this setting only if your network or application behind Enterprise Edge is diffserve capable or diffserve aware. Specify here the DS Code or TOS value that the application or the other edge device puts in the IP packets it sends. Otherwise, ignore this setting.

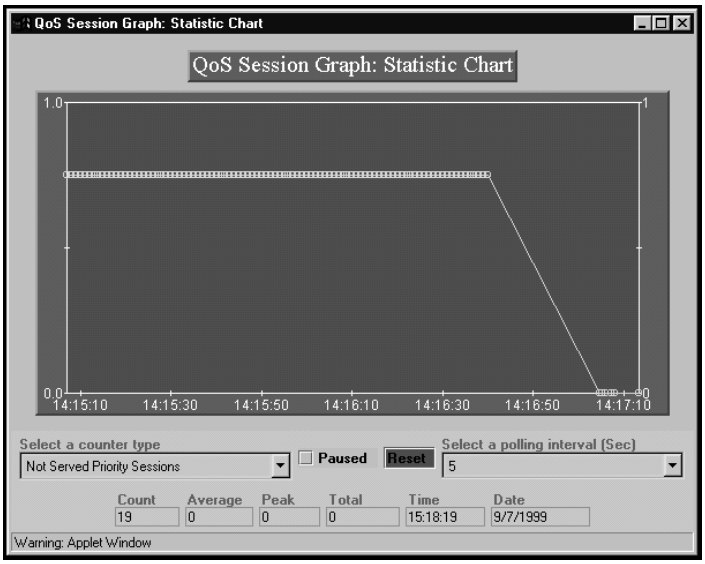
Setting	Definition
Priority	Lets users specify the priority given to packets that match the criteria specified in the filter. The priority value has significance only within the IP interface the packet is related, and is relative to other packets that go out through the interface. 0 is the highest priority and 8, the lowest priority. Use caution when you assign priority. If you assign priority 0 for regular data traffic, it is possible that the quality of voice calls that go through this interface are degraded. Use priority 0 only if your WAN does not carry any voice calls. As a guideline, always start assigning priorities from the lowest level up.
Outbound DS Code	Lets users specify the new DS Code added to the packets that match this filter. If you don't want to change the DS Code in the packets going out through the interface, don't specify any value for this setting. If a value is specified, this setting lets Enterprise Edge change the DS code on outgoing packets. This lets Enterprise Edge be used as a 'marker' device on the edge of a diffserve capable network.

2. In the **Description** box type the description.
3. In the **Version** box type the version.
4. From the **Status** list box select enable or disable.
5. In the **Premium Bandwidth** box type the appropriate premium bandwidth.
6. From the **Video Class** list box select the video class.
7. In the **Premium DS Code** box type the premium DS code.
8. In the **Number of Phone Ports** box type the number of phone ports.
9. Press the **Tab** key to save the settings.

QoS performance graphs and tables

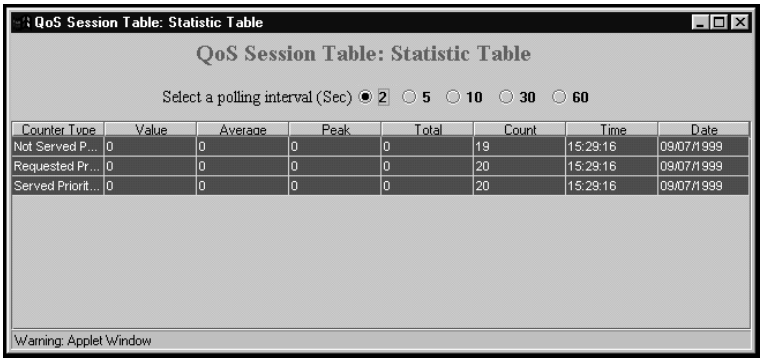
To access QoS performance graphs and tables:

1. On the menu, click **Performance** and then click **QoS Session Graph**. The QoS Performance Graph appears.



For information on using performance tables and graphs, refer to Graphs and tables on page 154.

2. On the menu, click **Performance** and then click **QoS Session Table**. The QoS Performance Table appears.



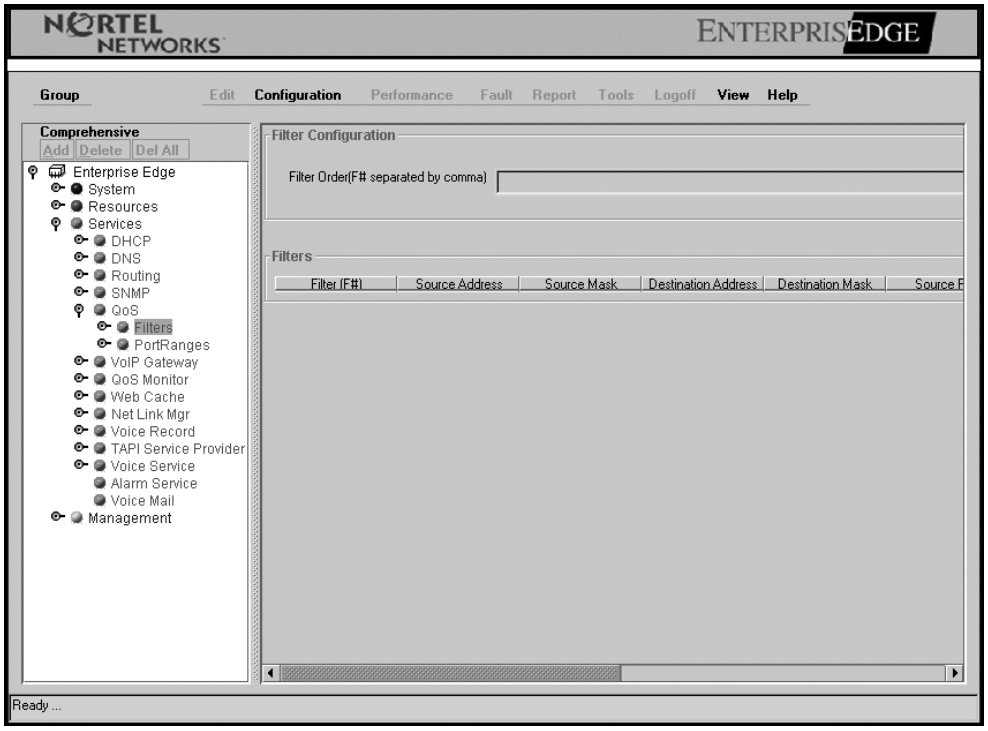
3. Access the remaining QoS graphs and QoS tables by following the steps for QoS Session Graphs and Tables.

QoS filters

To set the QoS filters:

1. Click the **QoS** navigation key to expand the navigation tree.

2. On the navigation tree, click **Filters**.
   Clicking the Filters navigation key causes the key to disappear. You must choose Filters. The Filters Configuration and Filters screen appears.



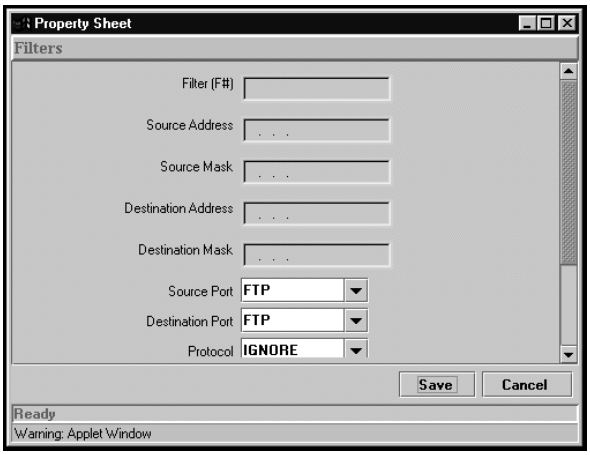
3. In the **Filter Configuration** box type the filter configuration.

4. Press the **Tab** key to save the settings.

To modify filters:

1. In the Filter table, click the filer you want to modify.

2. On the menu, click **Configuration** and then click **Modify Filter**.
   The Filters dialog box appears.



3. Make changes to any setting that you want to modify.

4. Click the **Save** button to return to Unified Manager.

To add filters:

1. On the menu, click **Configuration** and then click **Add Filter**.
   The Filters dialog box appears.

2. In the **Filter** box type the appropriate filter.
   Type a name that looks like “Fxx” where “xx” is a unique integer in the filter table.

3. In the **Source Address** box type the source address if it is required or leave this box empty.

4. In the **Source Mask** box type the source mask.
   If you specify a source address, you must specify a source mask.

5. In the **Destination Address** box type the destination address if it is required or leave this box empty.

6. In the **Destination Mask** box type the destination mask or leave this box empty.

7. From the **Source Port** list box, if required, select the source port or select ignore.

8. From the **Destination Port** list box select the destination port.

9. From the **Protocol** list box if required, select the protocol or click ignore to ignore this field.

10. In the **DSCode (TOS) Criteria** box select a DS code in hex or leave this setting blank.

11. From the **Priority** list box select the priority.
    Use caution when selecting a priority. Lower values have precedence over higher values. For priority 0, Enterprise Edge gives the same precedence as voice traffic, possibly affecting the latter adversely.

12. In the **Outbound DS Code (TOS)** box type the outbound DS code.

13. Click the **Save** button to return to Unified Manager.

To delete filters:

1. On the **Filter** table, click the filter you want to delete.

2. On the menu, click **Configuration** and then click **Delete Filter**.
   A message appears that asks you to confirm the deletion.

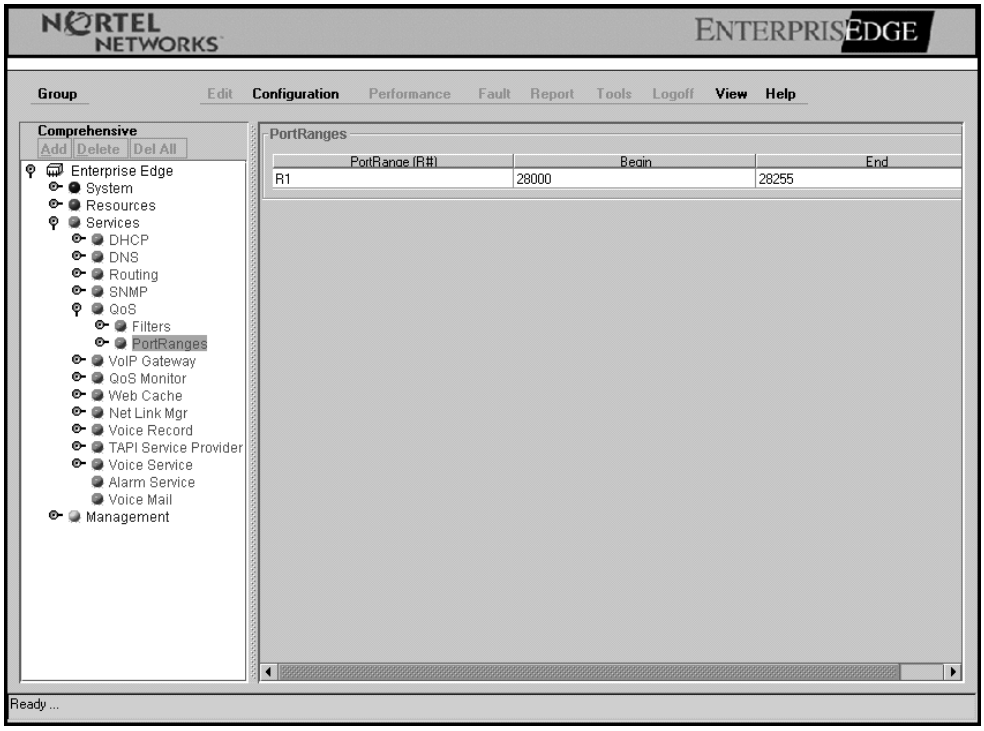
3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

QoS Port Ranges

4. Click the **QoS** navigation key.

5. On the navigation tree, click **PortRanges**.
   Clicking the Port Ranges navigation key causes the key to disappear. You must click PortRanges.

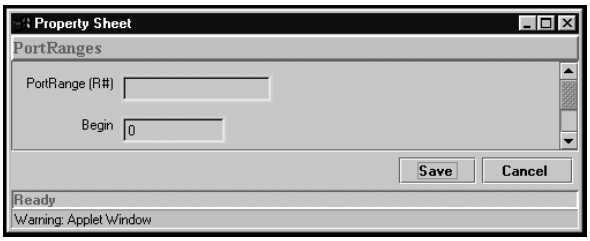
   The QoS PortRanges screen appears.



To modify port ranges:

1. In the **Port Ranges** table, click the port ranges you want to modify.

2. On the menu, click **Configuration** and then click **Modify Port Ranges**.
   The Port Ranges dialog box appears.



3. In the **Begin** box.type the beginning value for the range.
   This must be an even value.

4. In the **End** box type the appropriate end value for the range.

5. Click the **Save** button to return to Unified Manager.

To add port ranges:

1. On the menu, click **Configuration** and then click **Add Port Ranges**.
   The Port Ranges dialog box appears.

2. In the **PortRange** box type the port range.
   Type an entry that looks like “Rxx” where “xx” is a unique integer.

3. In the **Begin** box type the beginning value for the range.
   This must be an even value.

4. In the **End** box type the ending value for the range.

5. Click the **Save** button to return to Unified Manager.

   Note: If the rest of your network is not diffserv capable, you can set filters in other routers to give higher priority to VoIP traffic. In all the routers that carry VoIP traffic from the Enterprise Edge server, you must set filters that classify the traffic to and from these port ranges as high-priority.

To delete port ranges:

1. In the **Port Ranges** table, click the port ranges you want to delete.

2. On the menu, click **Configuration** and then click **Delete PortRange**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

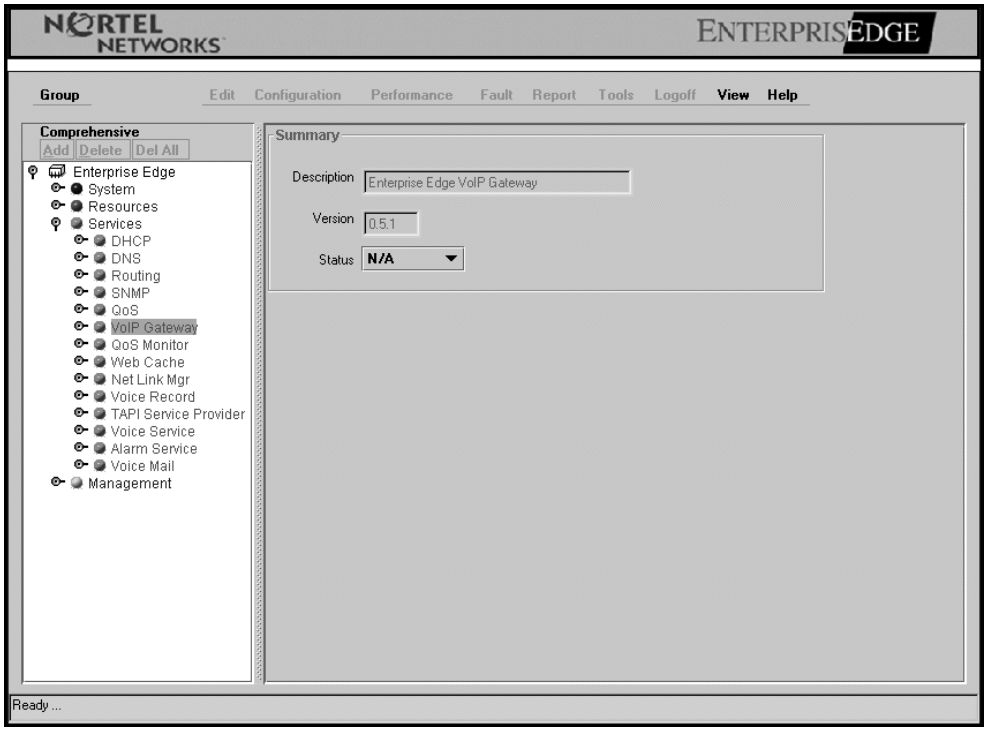
4. Click the **QoS** navigation key to close the navigation tree.

VoIP gateway

To configure VoIP gateway settings:

1. On the navigation tree, click **VoIP Gateway**.
   Clicking the VoIP Gateway navigation key expands the navigation tree but doesn't display the summary of configurable VoIP Gateway services. You must choose VoIP Gateway.

   The VoIP Gateway Summary screen appears.



The VoIP Gateway settings are:

Setting	Definition
Description	Shows the description of the VoIP gateway.
Version	Shows the version of the VoIP gateway.
Status	Lets users enable, disable, pause, or continue the VoIP gateway service.

2. From the **Status** list box select enable or disable.

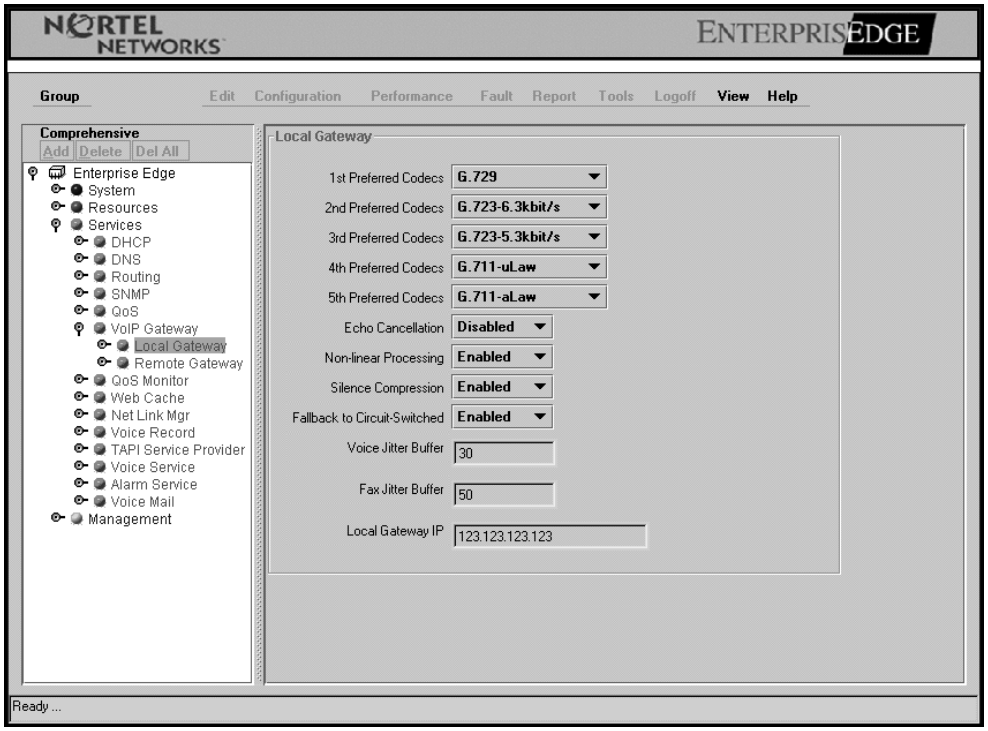
3. Press the **Tab** key to save the settings.

VoIP local and remote gateways

To configure VoIP local and remote gateways:

1. On the navigation tree click the **VoIP Gateway** navigation key to expand the navigation tree.

2. On the navigation tree click **Local Gateway**.
   Clicking the Local Gateway navigation key causes the key to disappear. You must click Local Gateway.



The VoIP Local Gateway settings are:

Setting	Definition
Preferred Codecs	Lets users specify the local VoIP gateway used to convert voice to data packets and vice versa. These parameters are always negotiated during call setup with the other VoIP gateway involved in the call. Codecs are negotiated in the order of preference specified here. Refer to the *VoIP Gateway User Guide* for a discussion on these values.
Echo Cancellation	Lets users enable or disable the Echo Cancellation feature in the VoIP calls.
Non-Linear Processing	Lets users enable or disable non-linear processing.
Silence Compression	Lets users enable or disable silence compression.
Fallback to Circuit Switched	Lets users enable or disable fallback to the circuit switched network (PSTN).

Setting	Definition
Voice Jitter Buffer	Lets users specify the voice jitter buffer size in the range of 20-200. The default setting is 50.
Fax Jitter Buffer	Lets users specify the FAX jitter buffer size in the range of 20-200. The default setting is 50.
Local Gateway IP	Lets users specify the local VoIP gateway to be used as its IP Address while interacting with other VoIP gateways. Since the Enterprise Edge server typically has more than one IP interfaces and more than one IP Address in it, users must choose one that VoIP gateway uses. This address must match the entry for this gateway in the remote gateway table of those VoIP gateways. Ensure this address is reachable to the other gateways via IP.

3. From the **1st Preferred Codecs** list box select the video class.

4. Configure the 2nd through 5th preferred codec selections.

5. From the **Echo Cancellation** list box enable or disable echo cancellation.

6. From the **Non-Linear Processing** list box enable or disable non-linear processing.

7. From the **Silence Compression** list box enable or disable silence compression.

8. From the **Fallback to Circuit-Switched** list box to enable or disable fallback to circuit-switched.

9. In the **Voice Jitter Buffer** box type the voice jitter buffer and press the **Tab** key.

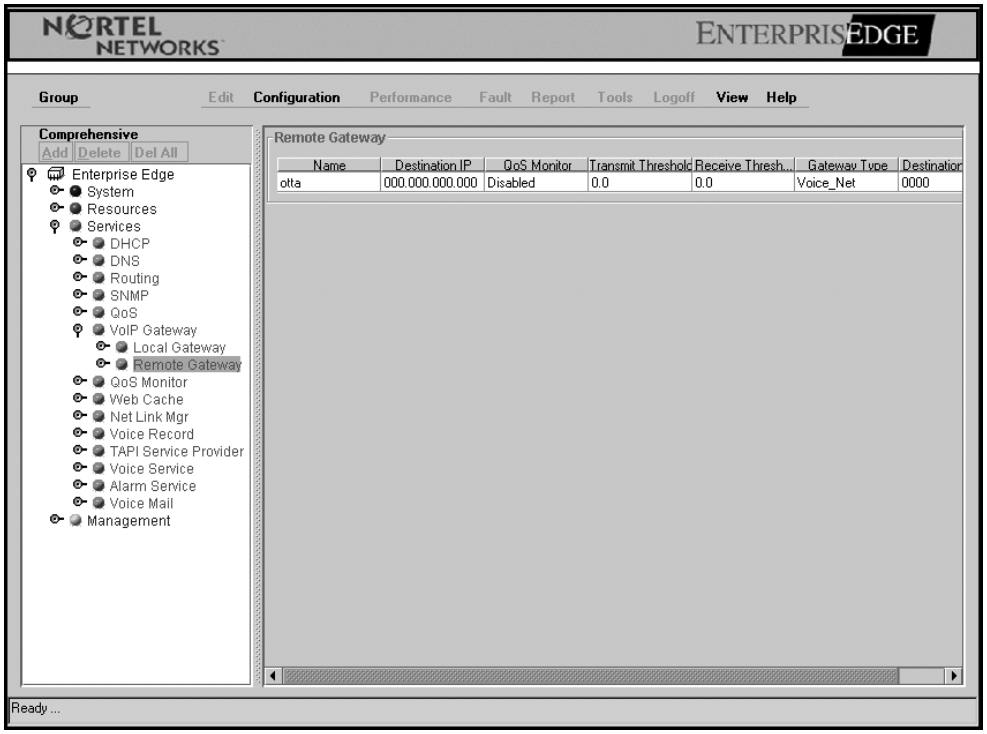
10. In the **Fax Jitter Buffer** box type the appropriate fax jitter buffer and press the **Tab** key.

11. In the **Local Gateway IP** box type the local gateway IP address and press the **Tab** key.

12. Press the **Tab** key save the settings.

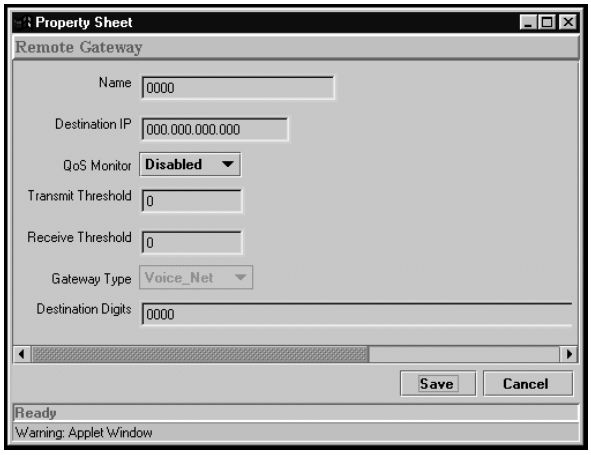
To modify VoIP Gateway Remote Gateway Entry services:

1. On the navigation tree, click **Remote Gateway**.
   Clicking the Remote Gateway navigation key causes the key to disappear. You must click Remote Gateway.
   The VoIP Remote Gateway screen appears.



1. In the **Remote Gateway** table, click the remote gateway you want to configure.

2. On the menu, click **Configuration** and then click **Modify Entry**. The Remote Gateway dialog box appears.



The VoIP Remote Gateway settings are:

Setting	Definition
Name	Lets users specify a logical name for the remote VoIP gateway. This setting is editable only when adding a new gateway entry. While modifying an existing entry, this name can not be changed.
Destination IP	Lets users specify IP Address for the remote VoIP gateway. Fully qualified DNS Name or just host name (where applicable) or IP address in dotted format may be entered here.
QoS Monitor	Lets users enable or disable QoS Monitor for this VoIP gateway.
Transmit Threshold	Lets users specify the transmit threshold that is used while interacting with this VoIP gateway.
Receive Threshold	Lets users specify the receive threshold that is used while interacting with this VoIP gateway.
Gateway Type	Lets users specify the VoIP gateway type. VoiceNet is the only permitted value in Release 1.0.
Destination Digits	Lets users specify the destination digits for this gateway. When the local gateway sees this prefix, it forwards the call to the VoIP gateway at the specified destination IP Address.

3. In the **Destination IP** box type the destination IP address and press the **Tab** key.

4. From the **Qos Monitor** list box enable or disable the QoS.

5. In the **Transmit Threshold** box type the transmit threshold and press the **Tab** key.

6. In the **Receive Threshold** box type the appropriate receive threshold.

7. In the **Destination Digits** box type the destination digits and press the **Tab** key.

8. Click the **Save** button to return to Unified Manager.

To add user profiles:

1. On the menu, click **Configuration** and then click **Add Entry**.
   The User Profile dialog box appears.

2. In the **Name** box type the user name.

3. In the **Destination IP** box type the destination IP address.

4. From the **Qos Monitor** list box enable or disable the QoS monitor.

5. In the **Transmit Threshold** box type the transmit threshold and press the **Tab** key.

6. In the **Receive Threshold** box type the receive threshold.

7. In the **Destination Digits** box type the destination digits.

8. Click the **Save** button to return to Unified Manager.

To delete remote gateways:

1. In the **Remote Gateway** table click the remote gateway you want to delete.

2. On the menu, click **Configuration** and then click **Delete Entry**.
   A message appears that asks you to confirm the deletion.

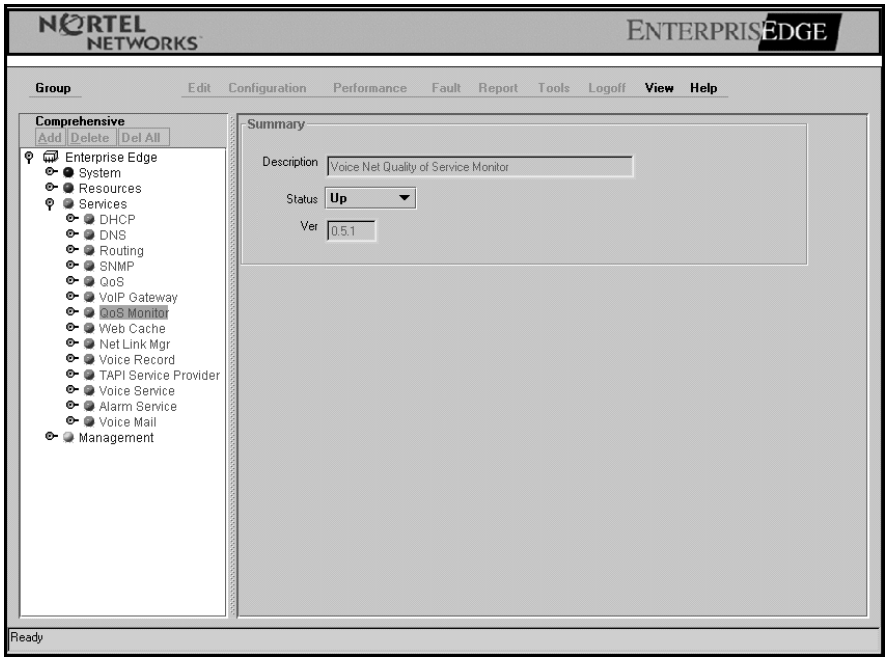
3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

4. Click the **VoIP Gateway** navigation key to close the navigation tree.

QoS monitor

To set the QoS monitor:

1. On the navigation tree, click **QoS Monitor**.
   Clicking the QoS Monitor navigation key expands the navigation tree doesn't display the summary of configurable QoS monitor services. You must click QoS Monitor.
   The QoS Monitor Summary screen appears.



The QoS Monitor settings are:

Setting	Definition
Description	Shows the description of the service monitor.
Version	Shows the version of the service monitor.
Status	Lets users enable or disable the service monitor.

2. From the **Status** list box select **enable** or **disable**.

3. Press the **Tab** key to save the settings.

QoS Monitor Mean Opinion Score

To view the QoS Monitor Mean Opinion Score:

1. Click the **Qos Monitor** navigation key.

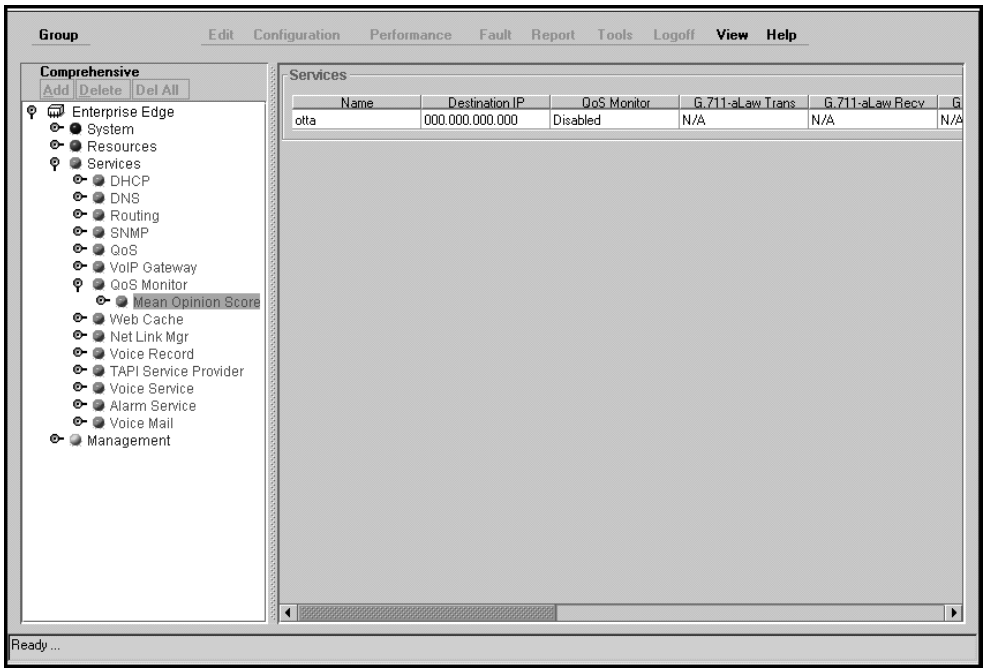
2. On the navigation tree, click **Mean Opinion Score**.
   Clicking the Mean Opinion Score navigation key causes the key to disappear. You must click Mean Opinion Score.

   If you configure or create remote gateways by clicking the Voice Net Remote Gateway navigation key, the mean opinion scores of the connections to these remote gateways, which are a measure of quality of the voice link, while using IP trunk, for each codec type are displayed in the screen. Each configured gateway appears on a separate row.

   Each row consists of the fields for the name of the remote gateway, its IP address, the status of the QoS monitoring for the connection, and the mean opinion scores for each allowed voice codec types and for each direction.

   If the QoS Monitor setting for the remote gateway entry is Disabled the MOS value for the remote gateway is N/A. Also, if the QoS Monitor service is disabled or down for any reason, all MOS values are N/A.

   While MOS values are being shown, they are updated approximately every 50 seconds. To refresh the data, on the menu click **View** and then click **Refresh**.

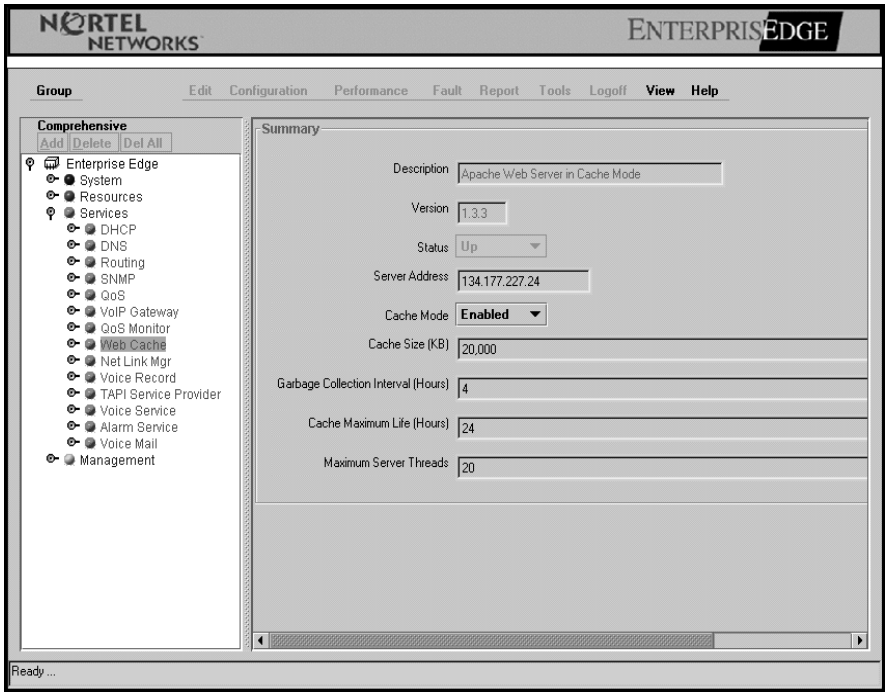


3. Click the **QoS Monitor** navigation key to close the navigation tree.

Web cache

To configure the web cache settings:

1. On the navigation tree, click **Web Cache**.
   The Web Cache Summary screen appears.



The web cache settings are:

Setting	Definition
Description	Shows the description of the Web Cache server.
Version	Shows the version of the Web Cache server.
Status	Shows the status of the Web Cache server. This setting is read-only. The server always runs r to provide support for web-based UIs for Enterprise Edge.
Server Address	Lets users tell the web server what IP address to use for interacting with HTTP clients. Since Enterprise Edge server typically has more than one IP interface and associated IP Address, users can choose this value. This value is automatically set to the IP Address of the first LAN interface and changes when the latter changes. Exercise caution if modifying this value
Cache Mode	Lets users enable or disable the cache-mode of operation.
Cache Size	Lets users specify the maximum size, in KB, of the cache.
Garbage Collection Interval	Lets users specify the interval, in hours, between garbage collection operations on the cache.
Cache Maximum Life	Lets users specify the maximum life on the proxy server for the HTTP pages cached in it.
Maximum Server Threads	Lets users specify the number of threads ready to serve HTTP requests in the proxy server.

2. In the **Server Address** box type the server address.
   This setting is automatically set to the LAN interface IP address. Use caution when changing.

3. From the **Cache Mode** list box select **enable** or **disable**.

4. In the **Cache Size** box type the cache size in KB.

5. In the **Garbage Collection Interval** box type the interval in hours.

6. In the **Cache Maximum Life** box type the cache maximum in hours.

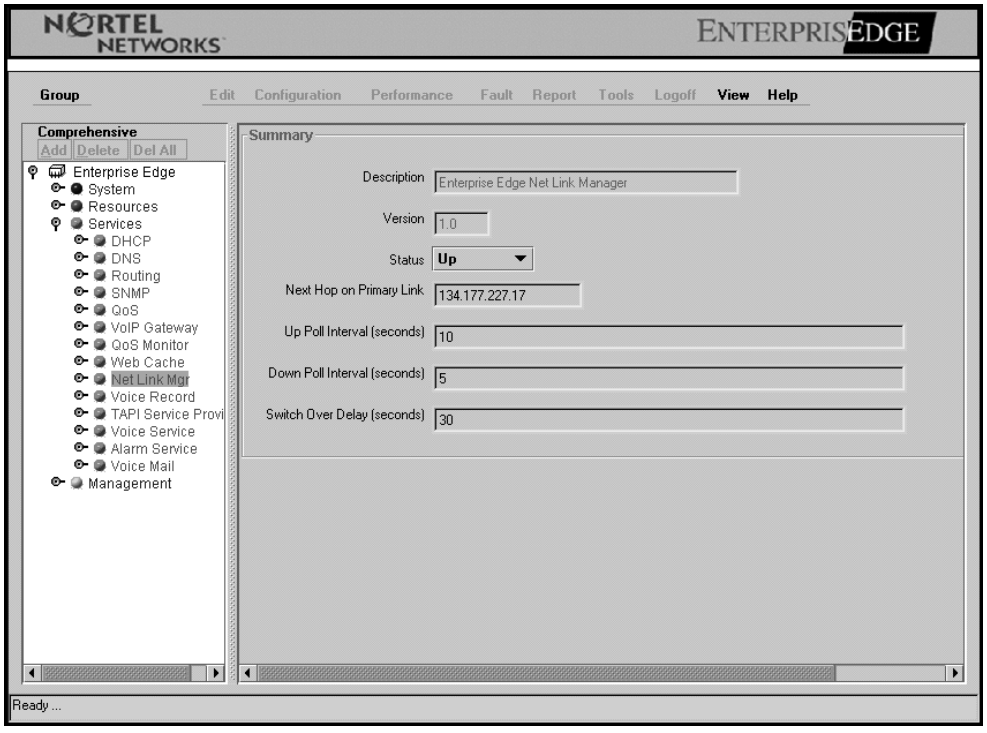
7. In the **Maximum Server Threads** box type the number of threads.

8. Press the **Tab** key to save the settings.

NetLink Manager

To configure NetLink Manager settings:

1. On the navigation tree click **NetLink Manager**.
   The NetLink Manager Summary screen appears.



The NetLink summary settings are:

Setting	Definition
Description	Shows a description of the Net Link Manager.
Version	Shows the version number of the subsystem.
Status	Shows the status of the Net Link Manager. The Net Link Manager is always running and cannot be disabled by the user.
Next Hop on Primary Link	Lets users specify the IP address in a valid dot format of the next hop router which is typically the remote router of the primary WAN data link.
Up Poll Interval	Lets users set the polling interval, in seconds, while the primary WAN data link is operational.
Down Poll Interval	Lets users set the polling interval, in seconds, while the primary WAN data link is down, and the dialup data link is operational.
Switch Over Delay	Lets users specify the interval, in seconds, that Net Link Manager waits for before switching the network link after it notices that the primary WAN link has come up again. This delay lets the router on the other end of the primary link recognize that the link has come up and adjust routing table accordingly. Typically this is set to the RIP Route Announcement Interval of 30 seconds.

2. From the **Status** list box select enable or disable.

3. In the **Next Hop on Primary Link** box type the “next hop.”
   This address is used by NetLink Manager to add a default route in the Enterprise Edge server. If this address is unreachable, NetLink Manager dials the backup link and changes the default route.

4. In the **Up Poll Interval** box type the up poll interval in seconds.
   The up poll interval is the interval between successive pings when the next hop in primary link is available. Use a relatively larger value to save bandwidth.

5. In the **Down Poll Interval** box type the down poll interval in seconds.
   The down poll interval is used to ping the next hop on primary link when it is recognized as unreachable. Use a smaller interval for faster recovery.

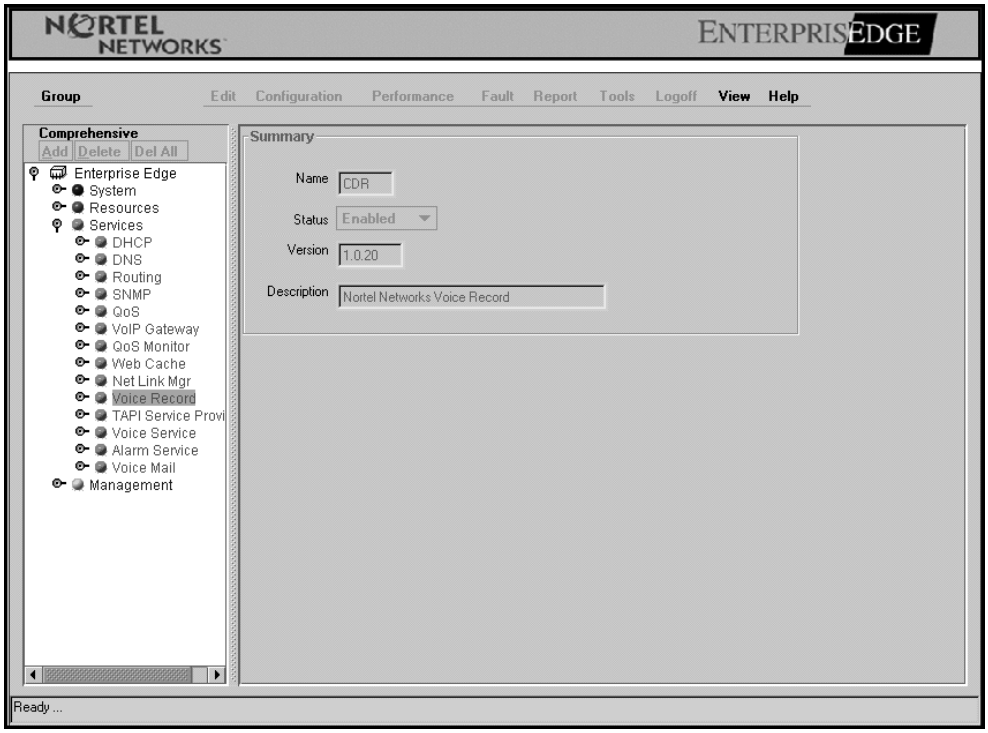
6. In the **Switch Over Delay** box type the switch over delay in seconds.

7. Press the **Tab** key to save the settings.

Voice Record

To configure Voice Record settings:

1. On the navigation tree click **Voice Record**.
   Clicking the Voice Record navigation key expands the navigation tree but doesn't display the read only summary. You must click Voice Record.
   The read only Voice Record Summary screen appears.



The Voice Record read-only settings are:

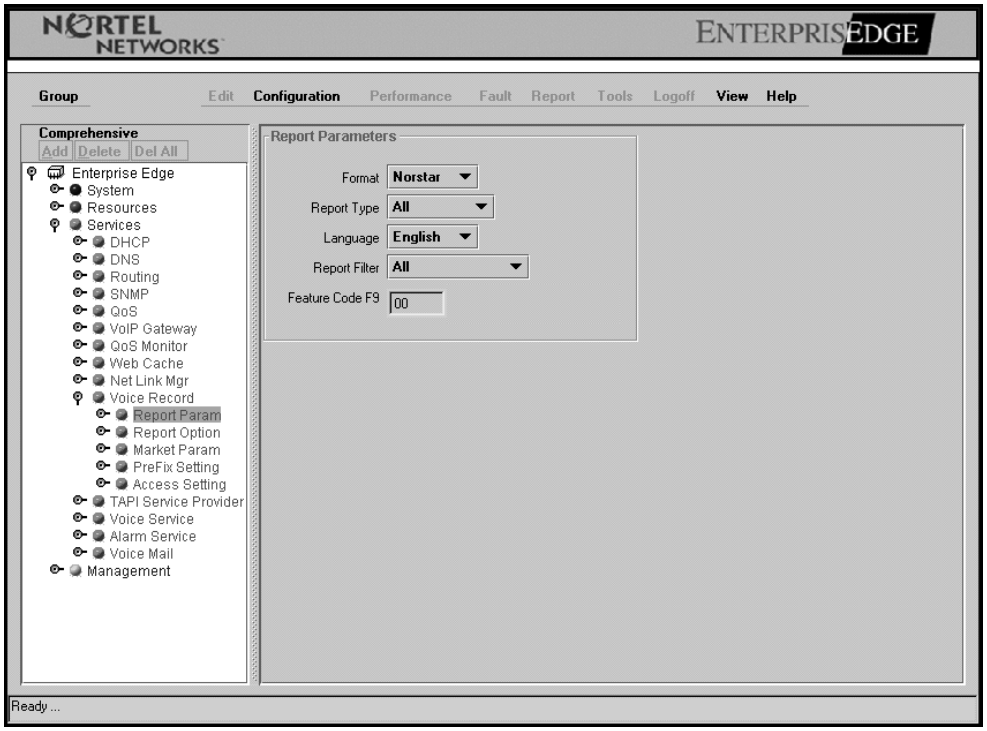
Setting	Definition
Name	Shows the component name, which is CDR.
Status	Shows the status of the component.
Version	Shows the version of the component.
Description	Shows a description of the component.

Voice Record report settings

To configure the Voice Record report settings:

1. On the navigation tree, click the **Voice Record** navigation key to expand the navigation tree.

2. On the **Report Parameters** from the navigation tree.
   Clicking the Report Parameters navigation key causes the key to disappear.
   You must choose Report Parameters.
   The Report Parameters screen appears.



The Voice Record report settings are:

Setting	Definition
Format	Lets user specify the record format from: SL-1 Norstar The default format is SL-1.
Report Type	Lets users select the report type from: Standard: Standard call information only CLID: Standard call information with CLID records Real time: Report real time call information for incoming calls only (available only when Norstar format is selected) All: Report standard call information with CLID records and real time call information (available only when Norstar format is selected) The default report type is Standard.

Language	Lets users select the language from: English French The default language is English
Report Filter	Lets users select the report filter type from: Outgoing: Report only outgoing calls. Incoming calls are not reported. Account Code: Reports only calls with account code stamped. Prefix: Report only calls with digits matched that long distance code in the prefix table. All: Reports all calls The default report filter is All.
Feature Code F9	Lets users specify the Feature Code F9 setting.

3. From the **Format** list box select the format.
4. From the **Report Type** list box select the report type.
5. Click the **Language** list box select the language.
6. From the **Report Filter** list box select the report filter.
7. From the **Feature Code F9** box select the feature code.
8. Press the **Tab** key to save the settings.

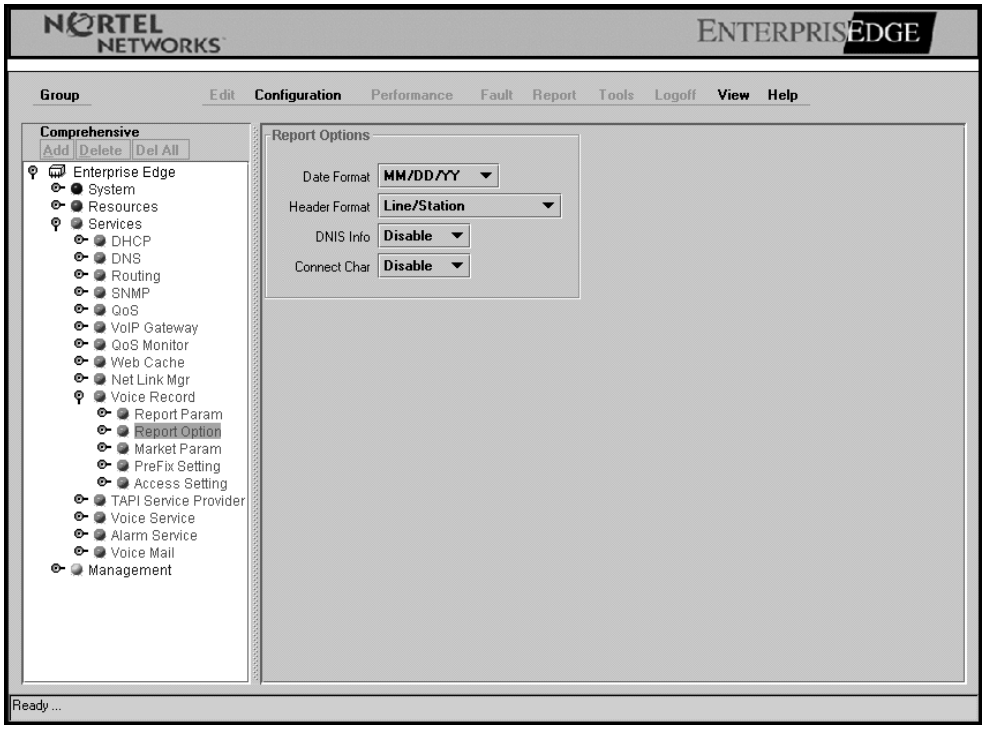
To configure commit and clip files:

1. On the menu, click **Configuration** and then click **Commit**.

Voice Record report options

To set Voice Record report options:

1. On the navigation tree, click **Report Options**.
   Clicking the Report Options navigation key causes the key to disappear. You must click Report Options.
   The Report Options screen appears.



The Voice Record report options are:

Setting	Definition
Date Format	Lets users specify the date format on voice mails recorded from: MM/DD/YY DD/MM/YY YY/MM/DD The default date format is MM/DD/YY.
Header Format	Lets users specify the header format for the recorded messages from: Line/Station: always reports the Line number first followed by the station number. Source/Destination: reports the source of the call followed by the destination of call. Incoming calls are reported in Line/Station format. Outgoing calls are reported in Station/Line format. The default header format is Line/Station format. This parameter affects only the Norstar record format.

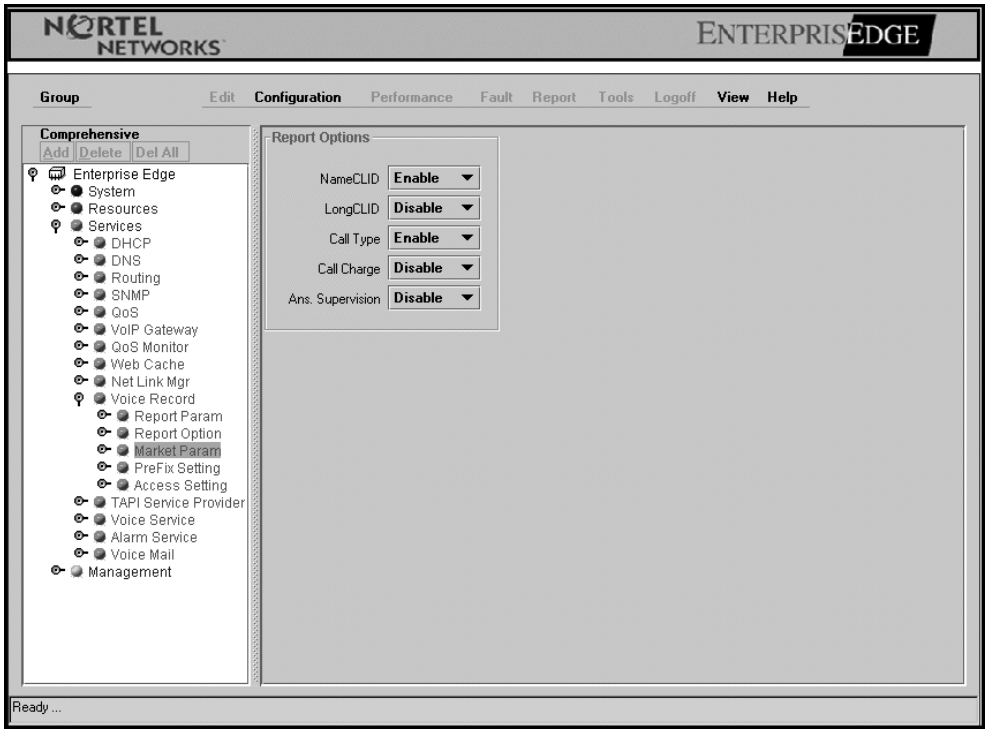
DNIS Info	Lets users enable and disable reporting Dialed Number Information Service (DNIS) digits. The default DNIS Info is Enabled This parameter affects only the Norstar record format. Not all trunks support DNIS.
Connect Char	Lets users enable and disable inserting "!" between digits dialed and after the call is connected. The default connect char is Disabled.

2. From the **Date Format** list box select a date format.
3. From the **Header Format** list box select a header format.
4. From the **DNIS Info** list box select enable or disable.
5. From the **Connection Character** list box select a connection character.
6. Press the **Tab** key to save the settings.

Voice Record market parameters

To set the Voice Record market parameters:

1. On the navigation tree, click **Market Parameters**.
   Clicking the Market Parameters navigation key causes the key to disappear. You must click Market Parameters.
   The Voice Record Market Parameters (report options) screen appears.



The Voice Record market parameters are:

Setting	Definition
NameCLID	Lets users enable and disable reporting the CLID Name of the call. This parameter affects only the Norstar record format. Not all trunks support CLID Name. The default NameCLID is Enabled.
LongCLID	Lets users enable and disable supporting the long CLID digit reporting. This parameter is very market specific. Do not change the default unless the trunk supports this feature. The default Long CLID is Disabled.
Call Type	Lets users enable and disable reporting the call type (Long distant or Unknown). This parameter affects only the Norstar record format. Do not change the default unless the trunk supports this feature. The default call type is Enabled.

Call Charge	Lets users enable and disable supporting the call charge reporting. This parameter is very market specific. Do not change the default unless the trunk supports this feature. The default call charge is Disabled.
Ans Supervision	Lets users enable and disable using Answer Supervision to identify far-end answered outgoing calls. This parameter is very market specific. Do not change the default unless the trunk supports this feature. The default ans supervision is Disabled.

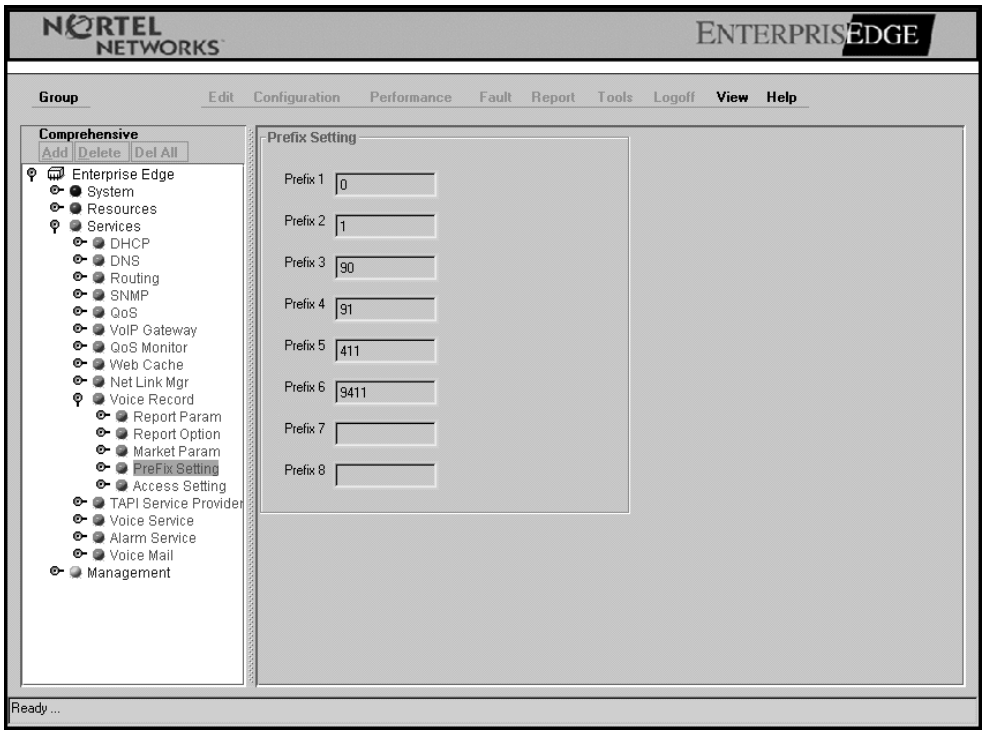
2. From the **NameCLID** list box enable or disable Name CLID.
3. In the **LongCLID** list box enable or disable Long CLID.
4. From the **Call Type** list box enable or disable call type.
5. From the **Call Charge** list box enable or disable call charge.
6. From the **Answer Supervision** list box enable or disable answer supervision.
7. Press the **Tab** key to save the settings.

Voice Record PreFix

The prefix setting lets users enter the long distance call prefixes in conjunction with the report filter option.

To set the Voice Record PreFix:

1. On the navigation tree, click **PreFix Setting**.
   Clicking the PreFix Setting navigation key causes the key to disappear. You must click PreFix Setting.
   The PreFix Setting screen appears.



2. In the **PreFix Setting** boxes type the appropriate prefixes.

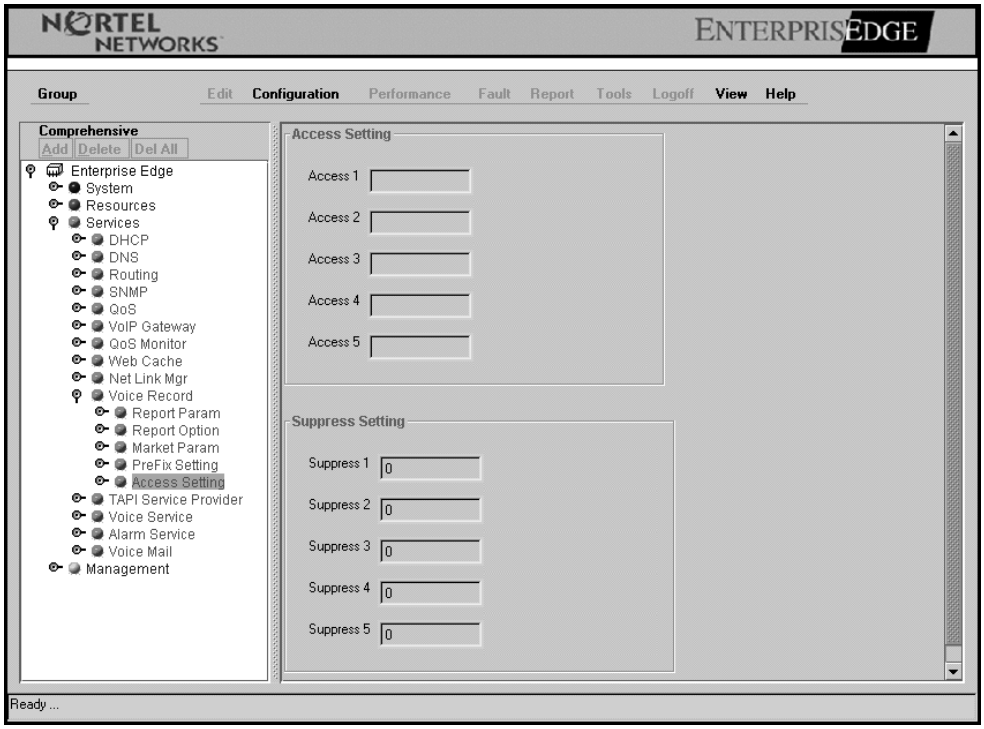
3. Press the **Tab** key to save the settings.

Voice Record Access/Suppress

To configure Voice Record Access/Suppress settings:

1. On the navigation tree, click the **Voice Record** navigation key.

2. On the navigation tree, click **Access Setting**.
   Clicking the Access Setting navigation key causes the key to disappear. You must click Access Setting.
   The Access Setting screen appears.



The Voice Record prefix settings are:

Setting	Definition
Access Setting	Lets users enter the secondary call provider call prefix digits.
Suppress Setting	Lets users enter the length of personal identification digits to suppress.

3. In the **Access and Suppress (access)** boxes type the appropriate access or suppress settings.

4. Press the **Tab** key save the settings.

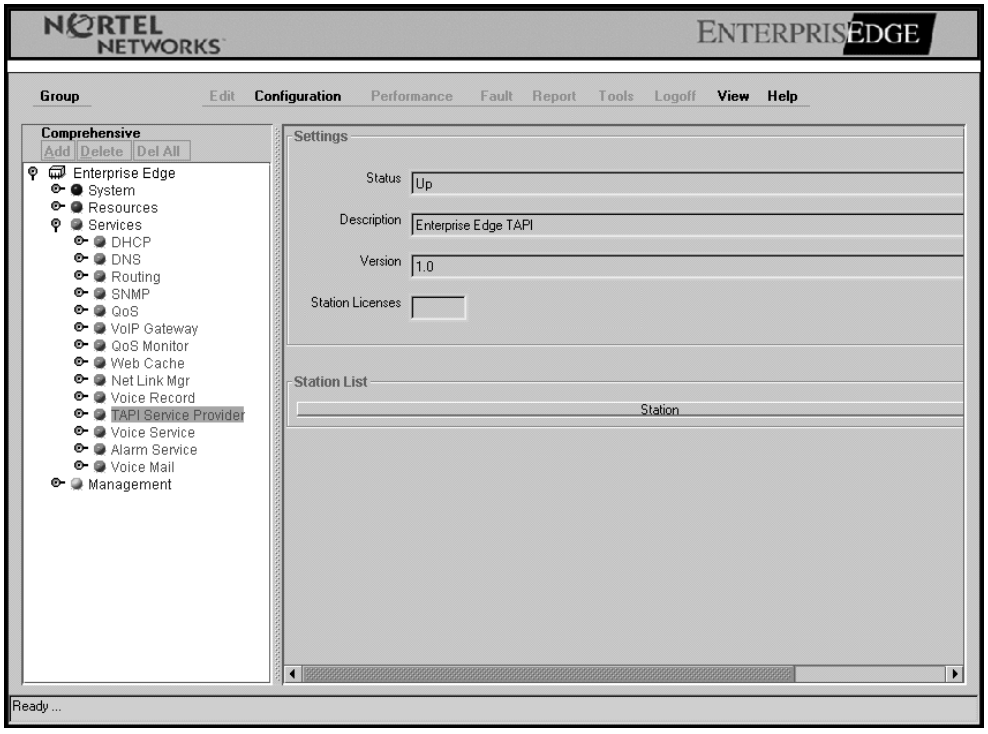
5. Click the **Voice Record** navigation key to close the navigation tree.

TAPI Service Provider

To configure TAPI Service Provider settings:

1. On the navigation tree, click **TAPI Service Provider**.
   Clicking the TAPI Service Provider navigation key causes the key to disappear, but doesn't show the read only settings. You must click TAPI Service Provider.
   TAPI Service Provider Settings and configurable Station List screen appears.

   TAPI Service Provider settings are read-only.



The TAPI Service Provider settings are:

Setting	Definition
Status	Shows the current status of the TSP (telephony service provider) as reported by the TSP software. The possible values are: Unknown In Service Not In Service Initializing In KSU Admin These strings are presented in English, French, or Spanish, depending on the software settings. The default value is Unknown and the typical value is In Service.
Description	Shows the description of TSP.

Setting	Definition
Version	Shows the TSP version.
Station Licenses	Shows the number of sets that are licensed to be controlled through the TSP. This is a numeric value or the text string Unlimited or Maximum. The station licenses can not be modified on this page but are changed by adding a keycode through the Software Keys page. The string Unlimited is presented in English, French, or Spanish. The default value is 2.
Station	Lets users add an internal phone number on the Enterprise Edge system. Users can add as many entries as there are licenses have been granted. The default is no entries in the Station List. List elements are added and deleted through the Configuration menu items.

2. On the menu click **Configuration** and then click **Add Station to List**. The Station List dialog box appears.

To add a station:

1. In the station box type the station information.

2. Click the **Save** button to return to Unified Manager.

To delete a station:

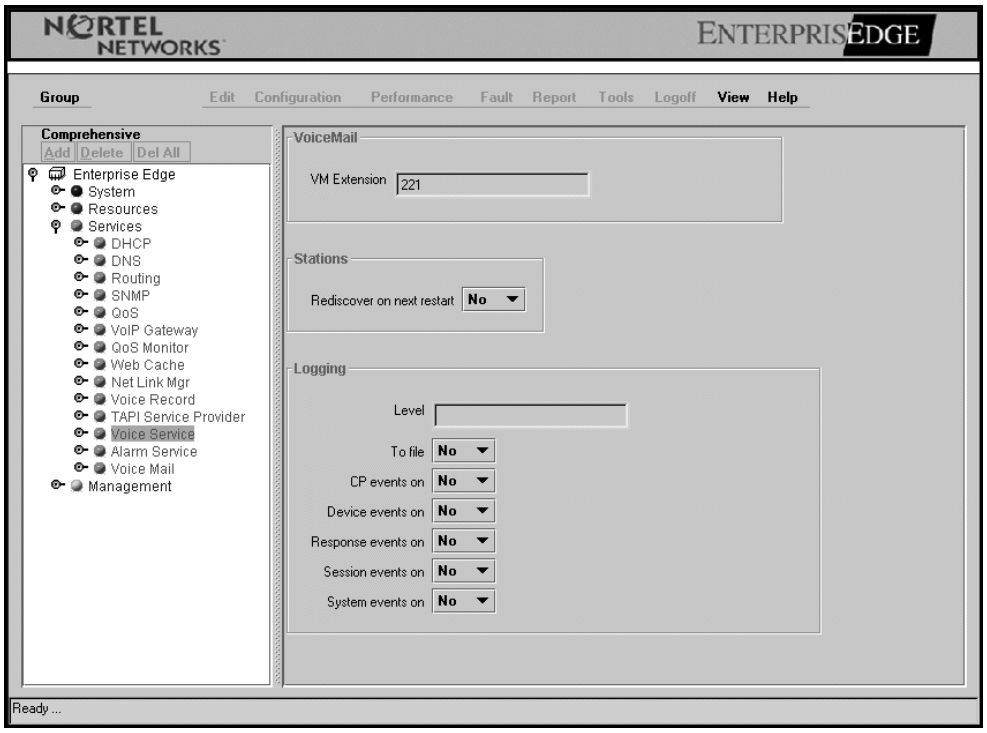
1. On the menu click **Configuration** and then click **Remove Station from List**. A message appears that asks you to confirm the deletion.

2. Click the **Yes** button to confirm the deletion and return to Unified Manager.

Voice Service

To configure Voice Service settings:

1. On the navigation tree click **Voice Service**.
   Clicking the Voice Service navigation key causes the key to disappear, but doesn't display the configurable summary. You must click Voice Service.
   The Voice Service VoiceMail, Stations, and Logging screen appears.



The Voice Service settings are:

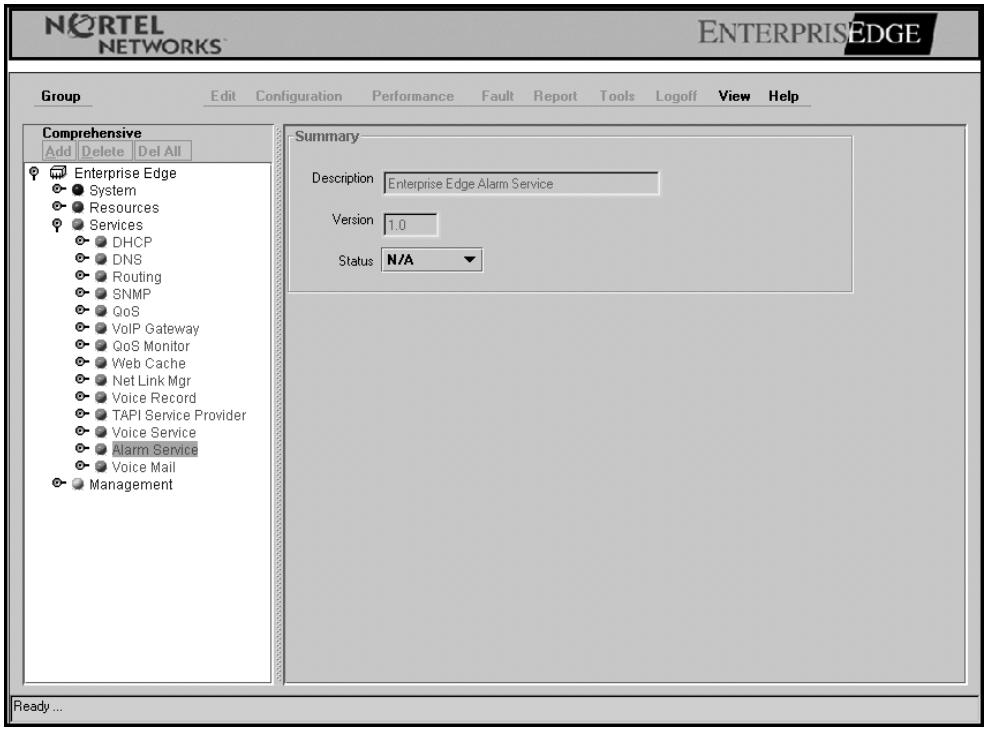
Setting	Definition
VM Extension	Lets users specify the default voice mail extension for the system. Specify an extension number for the voice mail system.
Rediscover on next restart	Lets users specify whether the system tries to communicate with all possible destination numbers to check for their status. Exercise caution before enabling this option as it can take up to 30 minutes to complete.
Level	Lets users specify the debug level. Any value between 0 and 20 is acceptable. The typical setting is 5.
To file	Lets users enable logging to the file. It enabled, it creates a file called ConsoleService.log on the file system.
CP Events Device Events Response Events Session Events System Events	Lets users enable events, including various types of events in the log file generated.

2. In the **VM Extension** box type the VM extension.
3. From the **Rediscover on next restart** list box select the answer.
4. In the **Level** box type the level.
5. From the **To File** list box select the answer.
6. From the **CP Events On** list box select the answer.
7. From the **Device Events On** list box select the answer.
8. From the **Response Events On** list box select the answer.
9. From the **Session Events On** list box select the answer.
10. From the **System Events On** list box select the answer.
11. Press the **Tab** key to save the settings.

Alarm Service

To configure Alarm Service settings:

1. On the navigation tree click **Alarm Service**.If you click Alarm Service the navigation key disappears. You must click Alarm Service.
   The Alarm Service Summary screen appears.



The Alarm Service summary settings are:

Setting	Definition
Descriptions	Shows a description of the alarm service.
Version	Shows the version of the alarm service.
Status	Lets users enable or disable the alarm service.

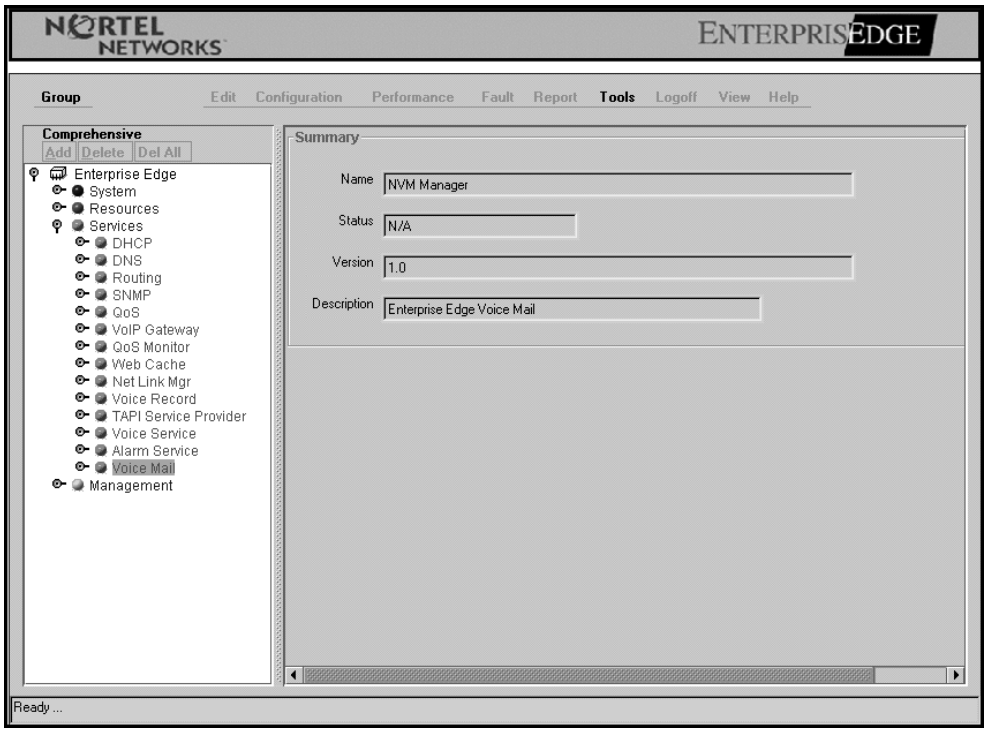
2. From the **Status** list box enable or disable alarm service.

3. Press the **Tab** key to save the settings.

Voice Mail

To configure Voice Mail services settings:

1. On the navigation tree click **Voice Mail**.
   Clicking the Voice Mail navigation key causes the key to disappear. You must choose Voice Mail.
   The Voice Mail Summary screen appears.



The Voice Mail settings are:

Setting	Definition
Name	Shows the name of the component.
Status	Shows the status of the voice mail service.
Version	Shows the version of the voice mail service.
Description	Shows the description of the voice mail service.

2. Click the **Services** navigation key to close the navigation tree.

Configuring Management Settings 7

Configuring Management Settings

When Enterprise Edge ships, the following user IDs are available:

- Manager: administrator user
- User: read-only user
- supervisor: administrator user

Note: After installation change the password for all administrator users or delete them after creating your own administrator users.

To configure management settings:

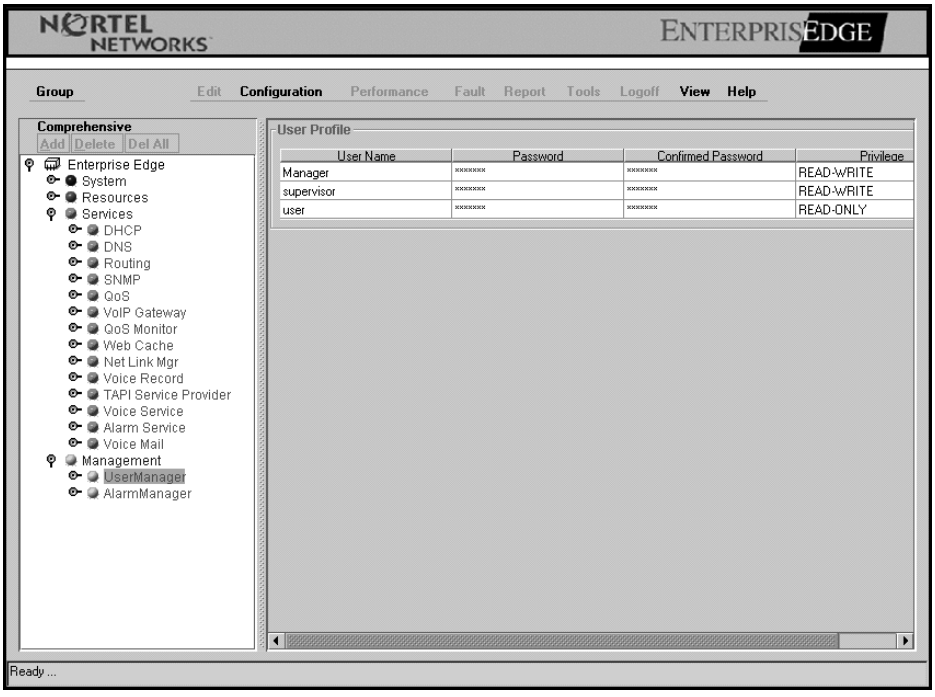
1. On the menu click **Group** and then click **Management** or **Comprehensive**.

2. On the navigation tree click the **Enterprise Edge** key and then click the **Management** key.

User Manager

To configure User Manager:

1. On the navigation tree click **User Manager**.
   Clicking the User Manager navigation key expands the navigation tree but doesn't display the User Manager management services. You must click User Manager. The User Manager User Profile screen appears.

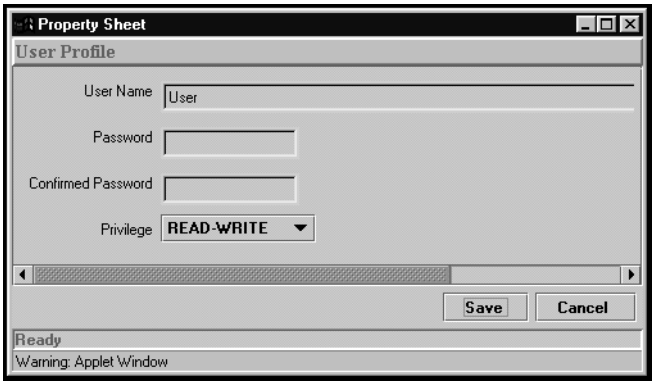


The User Manager settings are:

Setting	Definition
User Name	Lets users specify the user name while adding a new user. While modifying existing user profile, this field is read-only. The value in this setting is case sensitive and cannot exceed 50 characters in length.
Password	Lets users specify the password for the user. The value in this setting is case sensitive and cannot exceed 15 characters in length.
Confirmed Password	Lets users confirm the modified password. The value in this setting must match the value in the Password setting.
Privilege	Lets users specify what privileges this user has in administering the Enterprise Edge server from: READ-ONLY: Lets users view settings, but not alter them. READ-WRITE: Lets users view and change settings.

To modify user profiles:

1. In the **User Profile** table, click the user profile you want to modify.
2. On the menu click **Configuration** and then click **Modify User**.
   The User Profile dialog box appears.



3. In the **User Name** box type the user name.
4. In the **Password** box type the password.
5. In the **Confirmed Password** box retype the password.
6. From the **Privilege** list box select the appropriate user privilege.
7. Click the **Save** button to return to Unified Manager.

To add user profiles:

1. In the **User Profile** table click the line you want to configure.

2. On the menu click **Configuration** and then click **Add User**.
   The User Profile dialog box appears.

3. In the **Password** box type the password.

4. In the **Confirmed Password** box type the password.

5. From the **Privilege** list box.select the appropriate user privilege.

6. Click the **Save** button to return to Unified Manager.

   Note: Maintain only one user ID with administrative privileges with a few people allowed to use it. Multiple users logging on to Enterprise Edge from different client stations through the administrator account can causes inconsistent or wrong configuration. There is no security within Enterprise Edge to prevent it.

To delete user profiles:

1. In the **User Profile** table click the profile you want to delete.

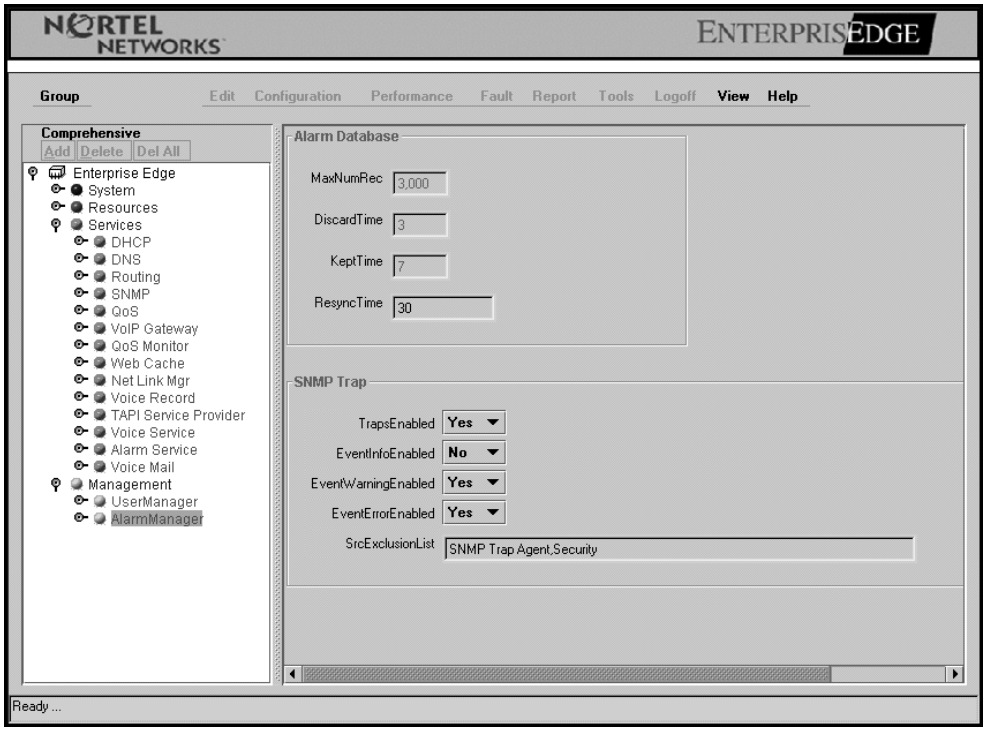
2. On the menu click **Configuration** and then click **Delete User**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

Alarm Manager

To configure alarm manager settings:

1. On the navigation tree click **Alarm Manager**.
   Clicking the Alarm Manager navigation key makes it disappear. You must click Alarm Manager.
   The screen displays Alarm Manager alarm database settings.



The Alarm Manager settings are:

Setting	Definition
Max Number Received	Shows the maximum number of records shown in the alarm database.
Discard Time	Shows the discard time, in seconds, for alarms. If the same alarm happens in this interval, it is discarded.
Kept Time	Shows the kept time, in days. An alarm is kept for this interval in the discard time database.
Resync Time	Shows the resync time, in seconds. Alarm service re-synchronizes with the event log at this interval. A value of 0 disables resynchronization.
Traps Enabled	Lets users enable or disable sending SNMP traps when a new event arrives to the event log.
Event Info Enabled	Lets users enable or disable sending SNMP traps for the events of 'Information' category.
Event Warning Enabled	Lets users enable or disable sending SNMP traps for the events of Warning category.

Setting	Definition
Event Error Enabled	Lets users enable or disable sending SNMP traps for the events of Error category.
ScrExclusion List	Lets users specify a comma-separated list of event sources whose events are not reported as SNMP traps. Depending upon the network and user environment, a component in Enterprise Edge may generate events of no significance to you at regular events. Adding that event's source name here prevents it from generating SNMP traps.

2. In the **Resync Time** box type the resync time.
3. From the **Traps Enabled** list box select **yes** or **no**.
4. From the **EventsInfoEnabled** list box select **yes** or **no**.
5. From the **EventWarningsEnabled** list box select **yes** or **no**.
6. From the **EventErrorEnabled** list box select **yes** or **no**.
7. In the **SrcExclusionList** box type the information.
8. Press the **Tab** key to save the settings.
9. Click the **Management** navigation key to close the navigation tree.

Diagnostics and Utilities 8

This chapter includes information Enterprise Edge diagnostics and utilities including:

- Uploading System Settings
- Downloading System Settings
- Enterprise Edge Performance Utility
- Error Messages
- MIB II Information

Saving System Settings

Enterprise Edge allows you to save the customized system settings for:

- Archival and backup purposes
- Downloading system settings to multiple Enterprise Edge units

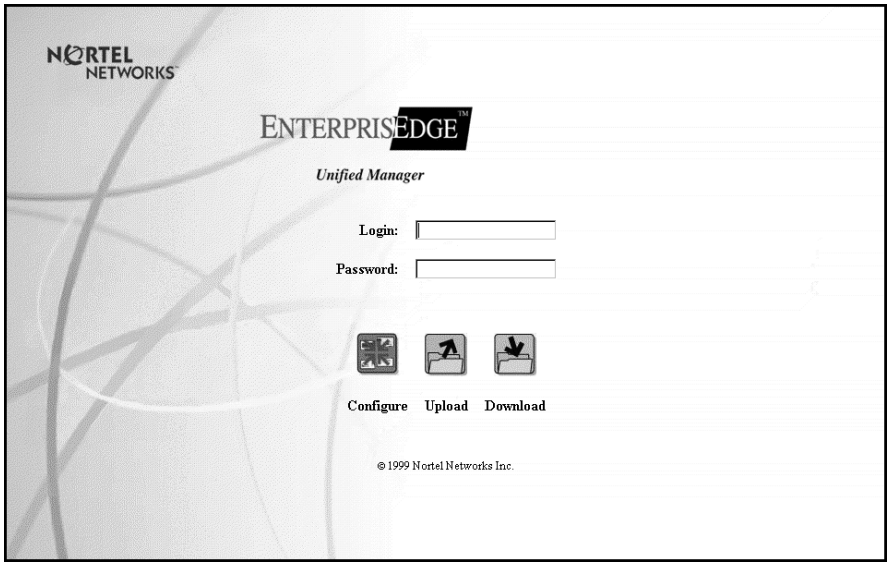
For example, you can use the download or upload feature to configure several Enterprise Edge servers by downloading definitions and uploading them onto new machines. This method of uploading definitions saves configuration time and can be used for archival and backup purposes.

Note: The upload feature is not supported in release 1.

Downloading System Settings

To download files:

1. On the log on screen, click the **Download** button.



   The download screen appears.

2. Select the underlined file and a download screens appears for the user to copy the file from the Enterprise Edge server to the user machine.

   The configuration files that you can download include the web user interface configuration and the subsystem configuration.

```
; $Workfile: webmenu.cfg $; $Revision: 41 $  ; $Date: 7/06/99 5:38p $
;=====================================================================
;
;               MSP   M A N A G E M E N T   S Y S T E M
;
;                  MSP WEB USER INTERFACE CONFIGURATION
;             Copyright (c) 1998,1999.  All rights reserved
;                        Bay Architecture Lab
;                        Nortel Networks, Inc.
;                     4401 Great America Parkway
;                        Santa Clara, CA 95054
;
;=====================================================================


; Templates
;=====================================================================
;=== XXXXXX Page Layout ==============================================
;=====================================================================
;=== Begin XXXXX Page Layout ====
;--- Page 1 Section ----------------
;--- Page 1 DropDown Menu ----------
;--- Page 1 Content ----------------
;--- Page 1 Window Content ---------
;=== End  XXXXX Page Layout ====

;#### Begin Configuration ##############################################

;=====================================================================
;=== Menu Tree Layout ================================================
;=====================================================================

;=== Begin Menu Main Level Layout ====

[MainMenu]
layout=menu,Menu
```

```
;$Header: /Management/Code/utils/config/subsys.cfg 90    8/05/99 3:28p Salse $

[ALL]
Provider=MSPSYS.DLL
Get=GetComponents
Set=SetModifiedTime

;no Set Method
;no Verify Method
;no Prepare Method
;no Apply Method

Fields=LastModified
;Components=SYSTEM,IP,DNS,DHCP,QoS,UserMgr,VOIP,QoSMon,VoCoder,VGtw,MOS,QMON,MSC,MscRcs,MscTel,Router,SNM
Components=SYSTEM,IP,DNS,DHCP,QoS,UserMgr,VOIP,QoSMon,VoCoder,VGtw,MOS,QMON,MSC,MscRcs,MscTel,Router,SNMP

Resources=LAN,WAN,MSC,MscRcs,MscTel,PBX
Services=DHCP,DNS,QoS,Router,SNMP,VOIP,QMON,Apache,WanLinkMgr,CDR,TSP,VoiceService,AlarmSvc

;Components=SYSTEM,IP,DNS,DHCP,WINS,ROUTER

[ClassMap]

;all sections are matched for only first 'n' characters, case-sensitive
CfgElement=ALL,SYSTEM,REBOOT,IP,IP-LAN,DNS,Router,Apache,
DynaFldElement=QoS,SNMP,IP-WAN,RTR-,UserMgr,VOIP,VGtw,MOS,MscRcs,MscTel,AlarmMgr,VoCoder,CDR,TSP,AlarmSvc
DhcpElement=DHCP

[DEFAULT]
;===Begin Attribute Setting ==========================================
DEFAULTLABEL=label,r,t,s,50,none
DEFSTAT=Disabled,rw,d,s,20,Enabled|Disabled
DEFSTAT2=Disabled,rw,d,s,20,Enabled|Disabled|Paused|Continue
DEFDESCR=none,r,t,s,100,none
DEFVER=none,r,t,s,50,none
;===End   Attribute Setting ==========================================
```

Graphs and tables

Enterprise Edge provides detailed performance information for the system and its components. The statistics are shown in charts or tables. If a performance display is active, it is automatically updated with real-time performance information in time increments that you set.

Note: Generating statistics puts a significant workload on the Enterprise Edge server CPU, connecting network, and web client. Exercise caution when running statistics for long durations.

Generating Statistics

Enterprise Edge provides statistical information on Enterprise Edge throughput and other performance-related information. The data is formatted in a chart or table format.

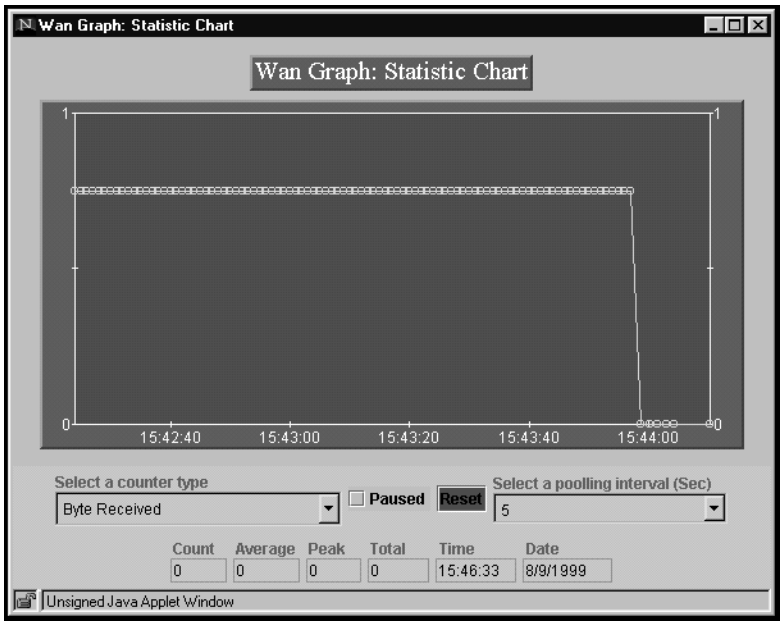
To generate statistics:

1. Select the appropriate item in the navigation tree.

2. Select **Performance** from the menu and select the appropriate command to display statistical information.z

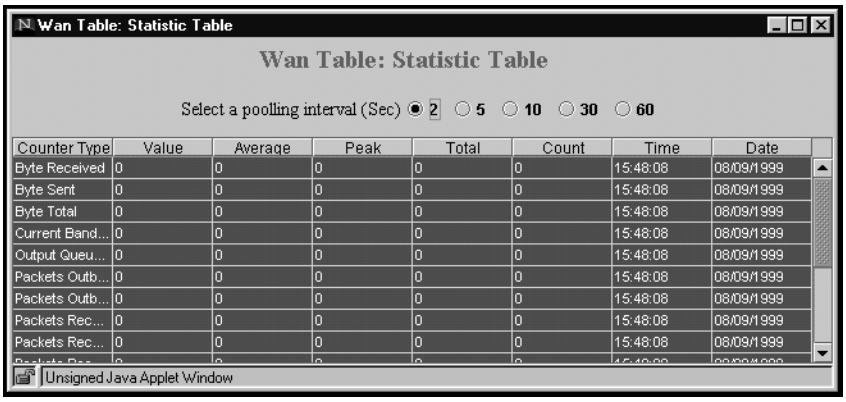
3. The chart or table appears.

Statistical Chart



The following is the same information in table format.

Statistical Table


Wan Table: Statistic Table
Wan Table: Statistic Table
Select a poolling interval (Sec) 2 5 10 30 60
Counter Type | Value | Average | Peak | Total | Count | Time | Date
Byte Received | 0 | 0 | 0 | 0 | 0 | 15:48:08 | 08/09/1999
Byte Sent | 0 | 0 | 0 | 0 | 0 | 15:48:08 | 08/09/1999
Byte Total | 0 | 0 | 0 | 0 | 0 | 15:48:08 | 08/09/1999
Current Band... | 0 | 0 | 0 | 0 | 0 | 15:48:08 | 08/09/1999
Output Queu... | 0 | 0 | 0 | 0 | 0 | 15:48:08 | 08/09/1999
Packets Outb... | 0 | 0 | 0 | 0 | 0 | 15:48:08 | 08/09/1999
Packets Outb... | 0 | 0 | 0 | 0 | 0 | 15:48:08 | 08/09/1999
Packets Rec... | 0 | 0 | 0 | 0 | 0 | 15:48:08 | 08/09/1999
Packets Rec... | 0 | 0 | 0 | 0 | 0 | 15:48:08 | 08/09/1999
Unsigned Java Applet Window

Sample Rate

You can set the sample rate by selecting the buttons on the statistical display. The polling intervals include 2, 5, 10, 30 and 60 seconds.

Error Messages

Messages appear if there is a system or processing error. The messages include two parts: the error string and the error number.

The error string includes the error description and the context of the error.

The error number is a three-part number that uniquely identifies the error. Be sure to note the error number when communicating with TSC to resolve the problem.

User Actions

Some Enterprise Edge errors are caused by a wrong parameter value. For these errors, the recommended action resolves the problem. Other possible errors are caused by an internal transition of states that puts the system and the user in an error condition. In this event, assistance from TSC is required to resolve the problem.

Note: Any Enterprise Edge errors that are not listed in this manual are advanced and require assistance from TSC for resolution.

Errors List

In the following list, in cases where multiple errors can happen in a particular context, a wild-card representation is used.

Error Number	Description	Action
2.5.4	This is an invalid data error. There was an error in setting system date. Reason: The date, month or year component contains a zero or negative value.	Provide the correct date value.
2.xx.4	These are various errors related to an error in setting system date Reason: The system rejected the date for various reasons. The reasons could be that it is beyond the range of dates supported. For example, 01/01/0001 is invalid date	
2.5.6	This is an invalid data error. There was an error in setting system time. Reason: The hour or minute component contains a negative value.	Provide the correct date value.
2.xx.6	These are various errors related to an error in setting system time	Correct the error in the time format.
2.5.8	This is an invalid data error. There was an error in setting system name. Reason: The system name does not follow the standard conventions.	Make sure that your system name does not contain any special characters in the name (hyphens are allowed, in addition to letters and digits), and that it does not exceed 15 characters in length.

5.4.59	This is an invalid configuration error. There was an error getting or setting DHCP parameters. Reason: You were adding an IP Address Range and/or Excluded Address Range and the first field you entered had a wrong key value. In the dialog boxes that appear to add the entries, the first field is a key that should match certain naming conventions. The conventions are given the label to those fields.	Follow the conventions given on the dialog boxes. For IP Address Ranges, use keys like 'Rxx' and for Excluded Address Ranges, use keys like 'Exx'
5.5.39	This is an invalid data value. There are invalid values for the new excluded address range. Reason: The IP Address values specified for the range are not correct. At present, each component in IP address specified in dotted format should be in the range 0-255, not including the boundary values.	Fix the value. If your IP Address range contains more than 255 addresses in it and you need to exclude a range that ends with 255 or starts with. 0, use the next upper or lower value to avoid specifying this value.
5.5.40	This is an invalid data value. There are missing values in the new excluded address range. Reason: Data for each excluded address entry should include two values - one for the start and the other for end. This error happens if one of them is missing.	Enter the missing value and click 'Save' again
5.5.41	This is an invalid data value. The new excluded address range is not completely within an IP Address range. Reason: Excluded Address ranges should be completely contained within a single IP Address range specified for the scope. If a DHCP scope contains more than one IP Address range, then the excluded address ranges specified, if any, may not span outside a single IP Address range in any way. This includes overhanging outside of a single IP Address Range or spanning over multiple IP Address Range.	Fix the over-hanging problem. If required, specify multiple excluded address range. Note: As a guideline, use only one IP Address range, and specify multiple excluded ranges to exclude disjoint parts of it.
5.5.45	This is an invalid data value. The new range overlaps with an existing range Reason: This error happens if the specified excluded range overlaps with another excluded address range or with an address that is already assigned to a DHCP Client computer.	Modify the new excluded address range so that it does not overlap with another or does not include assigned IP addresses. You may also go to the client system that go the assigned address and release IP address before setting the excluded range.

5.16.68	This is an invalid operation. You can't delete the last IP Address range in the scope. Reason: The scope contains only one IP Address range and you are attempting to delete it. You must have at least one IP Address range in the scope all the time. You may modify the last entry, however.	Don't delete the last DHCP range. If you need to change it, modify it. If you don't want the DHCP scope to be operational, change its status to 'Disabled'. If don't want any scope operational, set the status of the DHCP Service to 'Disabled'.
8.4.2.	This is an invalid configuration parameter. There was an error in setting data. Reason: You tried to add a port range or filter and the key field didn't contain the characteristic prefix.	If you are adding a new port-range, make sure the 'PortRange (R#)' field is like 'Rxx' where 'xx' is a number. If you are adding a new filter, make sure that 'Filter (F#)' field looks like 'Fxx' where 'xx' is a number.
8.5.3	This is an invalid data value. There was an error in setting port range Reason: You are setting a port range value and the upper and lower limits are not correct or missing.	Each range should begin with a positive even number and must end with a number greater than the beginning number and must be an odd number. Further, the range values should be less than 65535 (64K)
8.8.3	This is an error in data size. There was an error in setting port range. Reason: You are setting a port range that is too big. At present, only 256 ports can be set in the port-range table.	Consult chapter 3 for a discussion on port ranges in QoS. You may not need that big a range. Reduce it to be under 256 ports in the range.
9.4.2	This is an invalid configuration parameter. There was an error in setting data. Reason: This error can happen when you are setting a community string entry, manager entry or a trap community entry. Each entry uses a characteristic key string as its field name. Use 'Cxx' for community strings, 'Mxx' for manager entries and 'Txx' for trap community entries.	Use appropriate key strings in the dialog boxes, as suggested in their labels.
9.6.4 9.6.5 9.6.6	The object was not found. There was an error in setting <object Name> Reason: This error can happen while setting a community string entry, manager address or trap community entry. Each entry takes a characteristic key field as the first field that should follow certain conventions, and a unique number within the class. If that unique number is 0 or less, this error happens.	Specify correct number for the key field name.

10.5.2	This is an invalid data value for requested data. Reason: This can happen happens when user enters values into a dialog box and clicks 'Save' on it. If any of the fields had some strict format specified for it (say dotted format for an IP address) and if you entered a wrong value, it would beep when you tab out of the field. If you ignored that beep, the GUI would reject the field and when you clicked 'Save' it didn't send the field to the Enterprise Edge system, there by causing this problem.	Follow the rules precisely and pay particular attention to 'beeps.' If your IP Address has only 1 digit, prefix them with 0s in order to make them 3-digit in each segments of the dotted notation. If the screen has a scroll bar, scroll and enter all the necessary values.
11.5.2	This is an invalid data value for password. Reason: The user was changing a user profile and the password entered in 'password' and 'confirm password' fields do not match.	Match the passwords.
11.19.9	Failed to Delete. Required at least one user with read-write privilege. Reason: You are attempting to delete the last existing user with READ-WRITE privilege. This operation is not permitted, as it would not allow you to make any other changes to user configuration or other system configuration.	Add another user with read-write privilege before deleting the concerned user id.
11.12.10	Failed to Update. Required at least one user with read-write privilege. Reason: You are attempting to modify the last existing user with READ-WRITE privilege. At this time, no modifications are permitted to the last READ-WRITE user.	Add another user with READ-WRITE privilege before modifying the concerned user id.
14.4.21	Invalid Configuration Parameter. Error in setting interface parameter Reason: You're setting a static route, input filter or output filter under an interface and you didn't enter a correct characteristic key field in the dialog box. Values for these fields should strictly follow the convention provided in the labels for them. It should be something like 'SRxx' for static routes, 'IFxx' for input filters and 'OFxx' for output filters.	Make sure your key names are as per convention and provide unique values for the number component.

14.17.40 14.17.41	Command failed. Error in setting action for input/output filters Reason: You were attempting to set the action for input/output filters on the interface. The operation failed because, there were no input or output filters defined for the interface.	Add an input or output filter before setting the action
14.17.68	Command failed. Error is setting static route. This problem is caused by a mismatch in destination network address in its subnet mask specified in the route.	Match them. Bitwise 'AND' of destination address and subnet mask should be equal to the destination address.
	The routing protocol is changed and the screen didn't update.	Refresh the screen by clicking on 'View Refresh' menu item.
	The routing protocol for the interface shows up as 'RIP'. But no RIP configuration parameters show up on the screen	Set the routing protocol back to 'NONE' and then set to 'RIP' again. The RIP configuration field would show up.
14.5.77	Invalid Data Value. Static default route is not permitted in this version. Reason: You were setting a static route that was a default route for the system. In this release of Enterprise Edge, setting default routes as static routes is not permitted. The default route is managed by the 'Net Link Manager' component that accepts the address of next hop router on the primary and then adds or deletes (manages) the default route in the system.	None

MIB II Information

Here is the mapping between Enterprise Edge counters shown in statistics windows and standard MIB-II variables where applicable.

This section includes:

- Counters shown at LAN and WAN interface levels:
- ICMP Counters
- UDP Counters
- QoS Session Counters
- QoS Best Effort Traffic Counters
- QoS Dropped Packets Counter
- QoS Graph Counters
- QoS Best Effort Queue Counters

Counters Shown at LAN and WAN Interface Levels

1. Byte Received:	ifInOctets
2. Byte Sent:	ifOutOctets
3. Byte Total:	no equivalent (ifInOctets and ifOutOctets)
4. Current Bandwidth:	ifSpeed
5. Output Queue Length:	ifOutQLen
6. Packets Outbound Discarded:	ifOutDiscards
7. Packets Outbound Errors:	ifOutErrors
8. Packets Received Discarded:	ifInDiscards
9. Packets Received Errors:	ifInErrors
10. Packets Received Non-Unicast:	ifInNUcastPkts
11. Packets Received Unicast:	ifInUcastPkts
12. Packets Received Unknown:	ifInUnknownProtos
13. Packets Received:	no equivalent
14. Packets Sent Non-Unicast:	ifOutNUcastPkts
15. Packets Sent Unicast:	ifOutUcastPkts
16. Packets Sent:	no equivalent
17. Packets:	no equivalent

ICMP Counters

Note: Shown under Performance Menu under 'Resources':

1. Messages Outbound Errors:	icmpOutErrors
2. Messages Received Errors:	icmpInErrors
3. Messages Received:	icmpInMsgs
4. Messages Sent:	icmpOutMsgs
5. Messages:	no equivalent (icmpInMsgs + icmpOutMsgs)
6. Received Address Mask:	icmpInAddrMasks
7. Received Address Mask Reply:	icmpInAddrMaskReps
8. Received Destination Unreachable:	icmpInDestUnreachs
9. Received Echo Reply:	icmpInEchoReps
10. Received Echo:	icmpInEchos
11. Received Parameter Problem:	icmpInParmProbs
12. Received Redirect:	icmpInRedirects
13. Received Source Quench:	icmpInSrcQuenchs
14. Received Time Exceeded:	icmpInTimeExcds
15. Received Timestamp Reply:	icmpInTimestampReps
16. Received Timestamp:	icmpInTimestamps
17. Sent Address Mask:	icmpOutAddrMasks
18. Sent Address Mask Reply:	icmpOutAddrMaskReps
19. Sent Destination Unreachable:	icmpOutDestUnreachs
20. Sent Echo Reply:	icmpOutEchoReps
21. Sent Echo:	icmpOutEchos
22. Sent Parameter Problem:	icmpOutParmProbs
23. Sent Redirect:	icmpOutRedirects
24. Sent Source Quench:	icmpOutSrcQuenchs
25. Sent Time Exceeded:	icmpOutTimeExcds
26. Sent Timestamp Reply:	icmpOutTimestampReps
27. Sent Timestamp:	icmpOutTimestamps

UDP Counters

1. Datagrams No Port:	udpNoPorts
2. Datagrams Received Errors:	udpInErrors
3. Datagrams Received:	udpInDatagrams
4. Datagrams Sent:	udpOutDatagrams
5. Datagrams:	no equivalent (udpInDatagrams + udpOutDataGrams)

TCP Counters

1. Connection Failures:	tcpAttemptFails
2. Connections Active:	tcpActiveOpens
3. Connections Established:	tcpCurrEstab
4. Connections Passive:	tcpPassiveOpens
5. Connections Reset:	tcpEstabResets
6. Segments Received:	tcpInSegs
7. Segments Retransmitted:	tcpRetransSegs
8. Segments Sent:	tcpOutSegs
9. Segments:	no equivalent (tcpInSegs + tcpOutSegs)

QoS Session Counters

Note: These are proprietory counters implemented by QoS Provider Module.

1. Not Served Priority Sessions: The number of premium priority sessions declined by the QoS module - probably due to bandwidth restrictions.

2. Requested Priority Sessions: Total number of premium priority sessions requested

3. Served Priority Sessions: Number of premium priority sessions admitted.

QoS Best Effort Traffic Counters

Note: This is a proprietory counter.

1 = Total Best-Effort Octets: Total number octets carried in best-effort level

2 = Total Best-Effort Packets: Total number of packets carried in best-effort level.

QoS Dropped Packets Counter

Note: Proprietory counter in QoS.

1. Total Dropped Octets: Total number of octets dropped, probably due to insufficient buffer.

2. Total Dropped Packets: Total number of dropped packets.

QoS Graph Counters

1. Total Octets: Total number of octets sent by QoS

2. Total Packets: Total number of packets sent by QoS

3. Total Priority Octets: Total number of octets carried in premium priority.

QoS Best Effort Queue Counters

Note: This is a proprietory counter.

1. Total Queue XX Octets: Total number of octets carried at specified queue's priority.

2. Total Queue XX Packets: Total number of packets carried at specified queue's priority.

3. Total Queue XX Packets Dropped: Total number of packets dropped at specified queue - probably due to insufficient buffer space.

Appendix A: Troubleshooting

This chapter includes information on:

- How to Get Help
- Troubleshooting

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone Number
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Troubleshooting

For error message information see page. For other troubleshooting information, contact a Nortel Networks Technical Solutions Center.

Appendix B: Setting Up Remote Routers

This appendix includes example information on setting up Nortel Networks (BayRS) router and how to set up a range of UDP as a high priority.

This chapter includes:

- Creating an Outbound Traffic Filter
- Sample Criteria, Ranges, and Actions for UDP Filtering

Creating an Outbound Traffic Filter

To create an outbound traffic filter:

1. In the Configuration Manager window, click Circuits and then click Edits Circuits.
   The Circuit List window appears.

2. Select a circuit.

3. Click the **Edit** button.
   The Circuit Definition screen appears with the circuit you select highlighted.

4. Click **Protocols**, click **Edit Protocol Priority** and then click **Priority/ Outbound Filters**.
   The Priority/Outbound Filters window appears.

5. Click **Template**.
   The Filter Template Management window appears.

6. Click **Create**.
   The Create Priority/Outbound Template window appears.

7. Specify a descriptive name in the Filter Name field.

8. Click **Criteria**, click **Add**, click **Datalink**, click **IP** and then click **criterion**.
   The Add Range window appears. If you choose the User-Defined criterion, the Add User-Defined Field window appears first.

9. Type a minimum and maximum value to specify the range and click the **OK** button.
   The Add Range window closes. The new criterion and ranges now appear in the Filter Information field of the Create Priority/Outbound Template window.

10. Click **Action**, click **Add** and then click ***action***.

11. Click the **OK** button.
    The Filter Template Management window opens. The new template appears in the templates list.

12. Click **Done**.
    The Priority/Outbound Filters window opens.

13. Click **Create**.
    The Create Filter window opens.

14. Select a circuit in the Interfaces field.

15. Select a template in the Templates field.

16. Specify a descriptive name in the Filter Name field.

17. Click **OK**.
    The Priority/Outbound Filters window opens.

18. Click **Apply**.
    The filter is applied to the circuit.

Sample Criteria, Ranges, and Actions for UDP Filtering

The filtering goal is to place all VoIP H.323 traffic leaving a particular interface in the high priority queue. From the BayRS Site Manager:

Use a criteria path of **Criteria**, **Add**, **IP**, **IP**, **UDP Destination Port**

The range is 2065 to 2067.

The action path is: **Action**, **IP**, **Add**, **High Queue**.

Note: This example shows how to give H.323 traffic priority over other protocols on the interface.

Glossary

Term	Definition
address	A unique identifier assigned to networks and stations that allows each device to receive and reply to messages.
API	An application program interface (API) is the specific method prescribed by a computer operating system or by another application program that a programmer uses when writing an application program. The API is used to make requests of the operating system or another application. An API can be contrasted with a graphical user interface or a command interface (both of which are direct user interfaces) as interfaces to an operating system or a program.
ARP	The Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a physical machine address that is recognized in the local network. For example, in IP Version 4, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. The physical machine address is also known as a Media Access Control or MAC address. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.
asynchronous	A method of transmission where the time intervals between characters are not required to be equal and signals are sourced from independent clocks with different frequencies and phase relationships. Start and stop bits may be added to coordinate character transfer.
baud	The signaling rate of a line. The baud rate is the number of voltage or frequency transitions per second.
CHAP	The Challenge-Handshake Authentication Protocol (CHAP) is a method of establishing security on PPP links where the peers must share a plain text identifier. The caller sends a challenge message to its receiving peer and the receiver responds with a value it calculates based on the identifier. The first peer then matches the response with its own calculation. If the values match, the link is established. CHAP is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP).
client	A client is a computer system or process that requests a service of another computer system or process. A workstation requesting the contents of a file from a file server is a client of the file server.
dial-up connection	A dial-up connection is a temporary, as opposed to dedicated, connection between computers established over an analog or digital phone line.

DHCP	The Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization's network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.
DiffServ	Differentiated Services (DiffServ) is a implementation methodology for QoS service for IP networks. DiffServ is a rule based methodology intended to improve network performance. Instead of applying faster, more advanced technology, networks are managed by appropriate network policies. For DiffServ, there is a cost associated with higher quality services and a risk with lower quality services.
DLCI	The data link connection indentifier (DLCI) is used to identify a PVC in frame relay networks.
DNS	The domain name system or domain name server (DNS) is the system in the Internet that maps names of objects (most usually host names) into IP numbers or other resource record values. The namespace of the Internet is divided into domains, and the responsibility for managing names within each domain is delegated, typically to systems within each domain.
domain name	The domain name is used to organize Internet names into manageable groups, such as nortelnetworks.com.
Ethernet	Ethernet is a widely used LAN technology defined by the Ethernet and IEEE 802.3 specification for data transmission.
filtering	Filtering is the process of examining a data packet on the network to determine the destination of the data and to decide whether the packet should be passed along on the local LAN, copied to another LAN, or dropped.
frame	A frame is a unit of data transmission in a local area network.
frame relay	A frame relay is a high-speed, packet switching WAN protocol designed to provide efficient, high-speed frame or packet transmission with minimum delay. Frame relay uses minimal error detection and relies on higher level protocols for error control.
FTP	The file transfer protocol (FTP) allows a user on one host to access and transfer files to and from another host over a network. On the Internet, FTP refers to a tool for accessing linked files.
H.323	H.323 is the standard for sending voice (audio) and video using IP on the public Internet and within intranets.

HDLC	High-level Data Link Control (HDLC) is a group of protocols or rules for transmitting data between network points or nodes. In HDLC, data is organized into a unit (called a frame) and sent across a network to a destination that verifies its successful arrival. The HDLC protocol also manages the flow or pacing at which data is sent. HDLC is one of the most commonly-used protocols in what is Layer 2 of the industry communication reference model called Open Systems Interconnection (OSI).
host name	The host name is a readable name that uniquely identifies a device on the Internet and is associated with a corresponding IP address.
HTTP	The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the world wide web.
ICMP	ICMP is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses IP datagrams, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.
IETF	The Internet Engineering Task Force (IETF) is the committee that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society's Internet Architecture Board (IAB).
In-Band	In-band is a method of device access utilizing a network interface component within the device.
Internet-standard Network Management Framework	Device configuration and monitoring via SNMP.
IP	The Internet Protocol (IP) is the protocol that supports data being sent from one computer to another on the Internet. Each computer on the Internet has at least one address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into units called packets. Each of these packets contains both the sender's Internet address and the receiver's address. IP is a connectionless protocol, which means that there is no established connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.
IP address	The Internet Protocol address is a unique identifier that allows communication over the Internet to be directed to the appropriate destination. Every computer on the Internet must have a unique IP address. IP addresses are allocated by an ISP in following format: nnn.nnn.nnn.nnn, where nnn is a numeric value from 0 to 255. IP addressing might be referred to as being static (fixed) or dynamic.

ISDN	Integrated Services Digital Network (ISDN) is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install ISDN adapters (in place of their modems) can see highly-graphic web pages arriving at rates up to 128 Kbps.
LAN	A LAN is a network of interconnected workstations sharing the resources of a single processor or server within a relatively small geographic area.
MAC	The Media Access Control (MAC) is a physical address that is the portion of the data-link layer in 802.x networks that controls addressing information of the packet and enables data to be sent and received across a local area network.
Modem	A device that transmits signals over telephone lines. It converts binary electrical signals into acoustic signals, and vice versa.
multilink PPP	Multilink PPP is an extension to the PPP protocol that enables you to group a set of links into a bundle for more bandwidth. The links in the bundle can operate at different speeds. Typical links can be ISDN B channels, dial-up connections, and leased-lines.
name servers	A name server provides the means of translating readable host computer names into actual IP addresses so you do not have to remember long numbers to access other computers and destinations on the Internet. For example, DNS servers and WINS servers are name servers.
NetBIOS	The Network Basic Input/Output System (NetBIOS) is an interface and upper-level protocol developed by IBM for use with a proprietary adapter for its PC network product. NetBIOS provides a standard interface to the lower networking layers. The protocol provides higher-level programs with access to the network. Windows NT systems use NetBIOS.
Network Device	A network device is a hardware entity characterized by its use as a communications component within a networking infrastructure.
NIC	A network interface card (NIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a network. Personal computers and workstations on local area networks (LANs) typically contain a network interface card specifically designed for the LAN transmission technology, such as Ethernet or Token Ring. Network interface cards provide a dedicated, full-time connection to a network.
Out-of-Band	Out-of-band is a method of device access circumventing the network interface components within the device.
router	A router is a device that forwards traffic between networks, based on network layer information and routing tables. A router decides which path network traffic follows using routing protocols to gain information about the network and algorithms to choose the best route based on a routing matrix.

PAP	The Password Authentication Protocol (PAP) is a procedure used by PPP servers to validate a connection request. PAP works as follows: 1.After the link is established, the requestor sends a password and an id to the server. 2.The server either validates the request and sends back an acknowledgement, terminates the connection, or offers the requestor another chance. Passwords are sent without security and the originator can make repeated attempts to gain access. For these reasons, a server that supports CHAP will offer to use that protocol before using PAP.
Packet	A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, GIF file, URL request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into pieces of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When the packets have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end). A packet-switching scheme is an efficient way to handle transmissions on a connectionless network such as the Internet. An alternative scheme, circuit-switching, is used for networks allocated for voice connections. In circuit-switching, lines in the network are shared among many users as with packet-switching, but each connection requires the dedication of a particular path for the duration of the connection. *Packet* and *datagram* are similar in meaning. A protocol similar to TCP, the User Datagram Protocol (UDP) uses the term datagram.
PBX	A PBX (private branch exchange) is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office. The PBX is owned and operated by the enterprise rather than the telephone company (which may be a supplier or service provider, however).
PPP	The Point-to-Point Protocol (PPP) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation. PPP can process synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection.

protocol	A protocol is a formal set of communication rules developed by international standards bodies, LAN equipment vendors, or groups governing the format, control, and timing of network communications.
PVC	The permanent virtual circuit (PVC) is an end-to-end virtual connection in frame relay networks.
relaying	Relaying is the process of moving data along a path determined by a routing process. The data is relayed between a source and a destination.
remote (device)	A remote device is any network device that is accessible only by means of communication over a digital or analog (dial-up) network.
proxy	A proxy is a server that acts on behalf of another.
QoS	On the Internet and in other networks, Quality of Service (QoS) is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information. Using the Internet's Resource Reservation Protocol (RSVP), packets passing through a gateway host can be expedited based on policy and reservation criteria arranged in advance. Using ATM, which also lets a company or user preselect a level of quality in terms of service, QoS can be measured and guaranteed in terms of the average delay at a gateway, the variation in delay in a group of cells (cells are 53-byte transmission units), cell losses, and the transmission error rate. In Enterprise Edge, QoS is provided over IP. QoS is guaranteed for outgoing traffic until it reaches the next hop.
RAS	The remote access service (RAS) is the ability to get access to a computer or a network from a remote distance. In corporations, people at branch offices, telecommuters, and people who are travelling may need access to the corporation's network. Home users get access to the Internet through remote access to an Internet service provider (ISP). A remote access server is the computer and associated software that is set up to handle users seeking access to network remotely. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network.

RIP	The Routing Information Protocol (RIP) enables routers in the same autonomous system to exchange routing information by means of periodic updates. RIP is a widely-used protocol for managing routing information within a self-contained network such as a corporate local area network (LAN) or an interconnected group of such LANs. Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts is has on record) to its closest neighbor host every 30 seconds. The neighbor host passes the information to its next neighbor and so on until all hosts within the network have the same routing path information, a state known as network convergence. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination. RIP is considered an effective solution for small homogeneous networks. For larger, more complicated networks, RIP's transmission of the entire routing table every 30 seconds may put a heavy amount of extra traffic in the network. The major alternative to RIP is the Open Shortest Path First Protocol (OSPF).
SNMP	The Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their functions.
subnet mask	A value used to route packets on TCP/IP networks. When the IP layer has to deliver a packet through an interface, it uses the destination address contained in the packet, together with the subnet mask of the interface to select an interface, and the next hop in that subnet.
synchronous	A synchronous signal is sourced from the same timing reference. A synchronous signal causes the interval between successive bits, characters, or events to remain constant or locked in to a specific clock frequency.
TAPI	The Telephony Application Program Interface (TAPI) is a standard program interface that lets you and your computer communicate over telephones or video phones to people or phone-connected resources elsewhere in the world.
TCP	The Transmission Control Protocol is the major transport protocol in the Internet suite of protocols providing reliable, connection-oriented, full-duplex streams.
TCP/IP	The Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of networking protocols designed to link computers from multiple vendors.
Telnet	Telnet is a service that provides terminal-emulation capabilities for logging into the Enterprise Edge unit from a remote location.
Token-Ring	A token-ring is a network topology and data signaling scheme where a special data packet (called a token) is passed from one station to another along an electrical ring. A transmitting station takes possession of the token, transmits the data, then frees the token after the data has made a complete circuit of the electrical ring.
TOS	The type of service (TOS) field is located in the IP packet header and is used in DifServ processing.

UDP	The User Datagram Protocol (UDP) is a protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses IP. UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses IP to actually transfer a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.
VoIP	Voice over IP (VoIP) is the capability to deliver voice using the Internet Protocol. VoIP is a set of facilities for managing the delivery of voice information using the IP. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service. In addition to IP, VoIP uses the real-time protocol (RTP) to help ensure that packets get delivered in a timely way. Using public networks, it is difficult to guarantee Quality of Service (QoS). Using VoIP, an enterprise positions a VoIP device at a gateway. The gateway receives packetized voice transmissions from users within the company and then routes them to other parts of its intranet (local area or wide area network) or, using a T-1 or E-1 interface, sends them over the public switched telephone network.
WAN	A wide area network (WAN) is a geographically dispersed telecommunications network and the term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks.
Web cache	A web cache is a server or collection of servers that store copies of Internet content. The web cache server can be either located on the LAN where the clients it serves are also located, or it can be embedded within the enterprise WAN or at the client’s Internet Service Provider (ISP).
Web proxy (or HTTP proxy)	A web proxy is a server that acts on behalf of the requester of pages from an HTTP server and the Internet.
WFQ	Weighted Fair Queuing (WFQ) is a queuing method that allows low volume traffic such as Telnet to be given priority and interactive traffic receives higher priority than batch transfers. Also, high bandwidth usage traffic such as batch file transfer traffic gets equal priority with other high bandwidth use traffic.

Index

A

accessing the menu 17
accessing Unified Manager settings
  management 44, 147
  resources 44, 53
  services 44, 77
  system 44
address 171
Address Resolution Protocol (ARP) 171
adjusting views
  columns 13
  edges 13
  navigation tree 13
administration
  web based, setting up 21
admission control
  guidelines 35
  introduction 34
alarm manager settings
  overview 150
alarm service settings
  overview 144
API 171
application program interface 171
asynchronous 171

B

baud 171

C

cancel buttons 10
canceling changes 10
Challenge-Handshake Authentication Protocol (CHAP) 171
changes
  canceling 10
  storing 10
client 171
columns, changing the order of 15
command buttons, navigating with 9
configuration window
  element names 10
  save and cancel buttons 10
  scroll bars 10
  status indicator 10
  text fields 10
  window identifier 10
configuration windows, understanding 10
configuring Enterprise Edge
  dialog box window format 10
  edit in place format 10
  with edit in place 11
configuring management settings
  alarm manager
    overview 150
  introduction 147
  user manager
    overview 147
configuring resource settings
  introduction 53
  LAN 54
  MSC 74
  telephony 75
  WAN backup links
    access parameters 73
    link parameters 71
    overview 69
    summary parameters 70
  WAN primary links
    access parameters 60
    frame relay parameters 63
    line parameters 61
    overview 58
    performance graphs and tables 68
    PPP parameters 67
configuring service settings
  alarm service
    overview 144
  DHCP
    LAN 80
    overview 78
  DNS
    overview 86
  introduction 77
  NetLink manager
    overview 129
  QoS
    filters 115
    overview 110
    performance graphs and tables 114
    port ranges 118
  QoS monitor
    mean opinion score 127
    overview 126
  routing
    LAN 88
    overview 87
    WAN 101
  SNMP
    community list 105

manager list 105
overview 103
trap community list 105
Tapi service provider
overview 140
voice mail
overview 145
voice record
access/suppress settings 139
market parameters 136
overview 131
prefix settings 138
report options 134
voice service 142
VoIP Gateway 121
overview 120
Web cache
overview 128
configuring system settings
date 51
fault alarm banner 49
identification 51
introduction 44
name 45
performance graphs and tables 48
resource services 45
time 51
connecting to Enterprise Edge, methods for
remote dial-in 42

D

data link connection indentifier (DLCI) 172
date, system 51
DHCP 172
configuring automatically 28
guidelines 28
introduction 27
DHCP service settings
LAN 80
overview 78
diagnostics 153
dialog box window
format 10
dial-up connection 171
Differentiated Services (DiffServ) 172
DiffServ 172
DiffServ networks
introduction 33
packet marking 35
DLCI 172
DNS 172
gateway 29
guidelines 29
introduction 29
proxy 29
DNS service settings
overview 86
domain name 172
download system settings 154
Dynamic Host Configuration Protocol (DHCP) 172
dynamic IP addressing 25

E

edit in place
configuring with 11
format 10
element names 10
Enterprise Edge
administration, web-based, setting up 21
admission control 34
as a DHCP server 28
IP addresses, setting up
with a laptop 20
with a PC 20
IP routing
information protocol 26
specifics 25
static 26
LAN connections
overview 39
logging off 23
logging on 22
operational considerations 21
packet marking 35
powering down 23
rebooting 23
WAN connections
backup 41
overview 39
permanent 40
frame relay 40
PPP 40
error messages
10.5.2 161
11.12.10 161
11.19.9 161
11.5.2 161
14.17.40 162
14.17.41 162
14.17.68 162
14.4.21 161
14.5.77 162
2.5.4 158
2.5.6 158
2.5.8 158
2.xx.4 158
2.xx.6 158

5.16.68 160
5.4.59 159
5.5.39 159
5.5.40 159
5.5.41 159
5.5.45 159
8.4.2. 160
8.5.3 160
8.8.3 160
9.4.2 160
9.6.4 160
9.6.5 160
9.6.6 160
overview 158
system notification 10
user actions 158
Ethernet 172
LAN connections 39
WAN connections
backup 41
overview 39
permanent 40
frame relay 40
PPP 40

F

fast path routing 27
fault alarm banner settings 49
file transfer protocol (FTP) 172
filtering 172
criteria 170
ranges 170
filters
QoS 115
QoS, adding 116
QoS, deleting 117
QoS, modifying 116
frame 172
frame relay 40, 172
frame relay parameters, WAN 63
FTP 172

G

gateway, DNS 29

H

H.323 172
HDLC 173
help, customer support 167
High-level Data Link Control (HDLC) 173
host name 173
HTTP 173
HTTP proxy 178
Hypertext Transfer Protocol (HTTP) 173

I

ICMP 173
ICMP counters 164
identification, system 51
IETF 173
In-Band 173
information panel view 9
Internet Protocol (IP) 173
introduction 7
IP address 173
IP addresses, setting up
with a laptop 20
with a PC 20
IP addressing
dynamic 25
overview 25
static 25
IP routing
information protocol 26
introduction 24
overview 24
specifics 25
IP services
DHCP
configuring 28
ISDN 174

J

JAVA Virtual Machine (JVM) 21

L

LAN 174
LAN connections 39
LAN resource settings 54
LAN routing services 88
LAN to LAN fast path routing 27
LAN, DHCP settings 80
Legacy networks
introduction 33
port range settings 37
line parameters, WAN 61
link parameters, WAN 71
logging off of Enterprise Edge 23
logging on to Enterprise Edge 22
logon definitions
configure 23
download 23
login 23
password 23
upload 23

M

management settings, configuring 147
mean opinion score, QoS monitor 127
Media Access Control (MAC) 174

menu bar, navigating with 9
menu descriptions 17
MIB-II
  counters 163
  variables 163
modem 174
MSC settings 74
multilink PPP 174

N

name servers 174
name, system 45
navigation
  between views 14
  command buttons 9
  information panel view 9
  menu bar 9
  navigation keys 9
  navigation tree 9
  scroll bars 10
  TAB key 11
navigation keys, navigating with 9
navigation tree, navigating with 9
NetBIOS 174
NetLink manager settings
  overview 129
network device 174
network interface card (NIC) 174
NIC 174
Nortel Networks Technical Solutions Centers 167

O

operational considerations 21
outbound traffic filter, creating 169
Out-of-Band 174

P

packet 175
packet filtering
  features
    destination address 27
    destination mask 27
    destination port 27
    ICMP code 27
    ICMP type 27
    protocol 27
    source address 27
    source mask 27
    source port 27
  introduction 26
packet marking
  DiffServe networks 35
  TOS, premium traffic 35
  TOS, priority filters 35
parameters
  obtaining required values 19
  required values 19
parameters, configuring 10
Password Authentication Protocol (PAP) 175
PBX (private branch exchange) 175
performance 156
  statistics, generating 16
performance graphs and tables
  QoS 114
  system 48
  WAN 68
permanent virtual circuit (PVC) 176
Point to Point Protocol (PPP) 40
Point-to-Point Protocol (PPP) 175
port range settings
  Legacy networks, overview 37
port ranges
  QoS 118
  QoS, adding 119
  QoS, deleting 119
  QoS, modifying 118
  service settings 118
powering down Enterprise Edge 23
PPP 175
PPP parameters, WAN 67
protocol 176
protocols
  routing information 26
proxy 176
  DNS 29
  web caching 30

Q

QoS best effort queue counters 166
QoS best effort traffic counters 165
QoS dropped packets counter 166
QoS filters
  adding 116
  deleting 117
  modifying 116
QoS graph counters 166
QoS module
  relationship with the VoIP QoS monitor, overview 38
  restrictions and defaults 38
QoS monitor settings
  mean opinion score 127
  overview 126
QoS port ranges
  adding 119
  deleting 119
  modifying 118
QoS service settings 110

filter 115
performance graphs and tables 114
port ranges 118
QoS session counters 165
Quality of Service (QoS) 176
overview 32
R
RAS 176
rebooting Enterprise Edge 23
relaying 176
remote (device) 176
remote access service (RAS) 176
remote dial-in
guidelines 42
remote routers, setting up 169
resource services settings 45
resource settings, configuring 53
RIP 177
RIP, enabling on network interfaces 26
router 174
routing
LAN settings 88
settings 87
WAN settings 101
routing and IPservices 7
Routing Information Protocol (RIP) 177
routing, IP
information protocol 26
introduction 24
IP addressing overview 25
managing information 26
overview 24
packet filtering
introduction 26
RIP protocol 26
static 26
routing, LAN to LAN fast path 27
S
sample rate 157
save buttons 10
saving settings 153
scroll bars 10
services, configuring 77
services, IP
DHCP
configuring 28
setting up
JAVA Virtual Machine 21
logging off of Enterprise Edge 23
logging on to Enterprise Edge 22
operational considerations 21
powering down Enterprise Edge 23
rebooting Enterprise Edge 23
web-based administration 21
settings, saving 153
Simple Network Management Protocol (SNMP) 177
SNMP 177
guidelines 31
overview 31
SNMP service settings
community list 105
manager list 105
overview 103
trap community list 105
static IP addressing 25
static IP routing 26
statistics
charts 156
charts, generating 16
generating 156
sample rate 157
tables 157
tables, generating 16
statistics, generating 16
status indicator 10
storing changes 10
subnet mask 177
summary parameters, WAN 70
support 167
synchronous 177
system notification
error messages 10
system performance graphs and tables 48
system settings, configuring 44
system software 8
T
TAPI 177
Tapi service provider
overview 140
TCP 177
TCP counters 165
TCP/IP 177
technical support 167
Telephony Application Program Interface (TAPI) 177
telephony settings 75
Telnet 177
text fields 10
time, system 51
token-ring 177
TOS 177
premium traffic 35
priority filters 35

troubleshooting 167
type of service (TOS) 177

U

UDP 178
UDP counters 165
Unified Manager
  accessing menu 17
  adjusting views 13
  column order, changing 15
  configuring 10
  menu descriptions 17
  navigating 9
  navigating between views 14
  parameters, configuring 10
  statistics, generating 16
User Datagram Protocol (UDP) 178
user manager settings
  overview 147
utilities
  overview 153
  performance 156

V

views, navigation between 14
voice mail settings
  overview 145
voice record
  access/suppress settings 139
  market parameters settings 136
  prefix settings 138
  report options settings 134
  service settings 131
voice service settings 142
VoIP 178
VoIP gateway settings
  local gateway 121
  overview 120
  remote gateway 121
VoIP QoS Monitor
  relationship with the QoS module, overview 38

W

WAN bandwidth, for admission control 34
WAN connections
  backup 41
  overview 39
  permanent 40
    frame relay 40
    PPP 40
WAN resource settings
  backup links
    access parameters 73
    link parameters 71
    overview 69
    summary parameters 70
  primary links
    access parameters 60
    frame relay parameters 63
    line parameters 61
    overview 58
    performance graphs and tables 68
    PPP parameters 67
WAN routing services 101
web cache 178
Web cache settings
  overview 128
web caching/proxy
  guidelines 30
  introduction 30
web proxy 178
web-based administration, setting up 21
Weighted Fair Queuing (WFQ) 178
wide area network (WAN) 178
window identifier 10